MIT'S MAGAZINE OF INNOVATION

TECHNOLOGY REVIEW

AUGUST 2003

WWW.TECHNOLOGYREVIEW.COM

Wireless Sensor Networks

Biotech's Big Chill

Saving Lives with Living Machines

Teachable Robots

SPAM WARS

BY THE TIME YOU READ THIS, HALF OF ALL E-MAIL WILL BE JUNK—COSTING BILLIONS AND CLOGGING THE INTERNET. THE COUNTERATTACK HAS BEGUN.

PLUS Monitoring Seniors

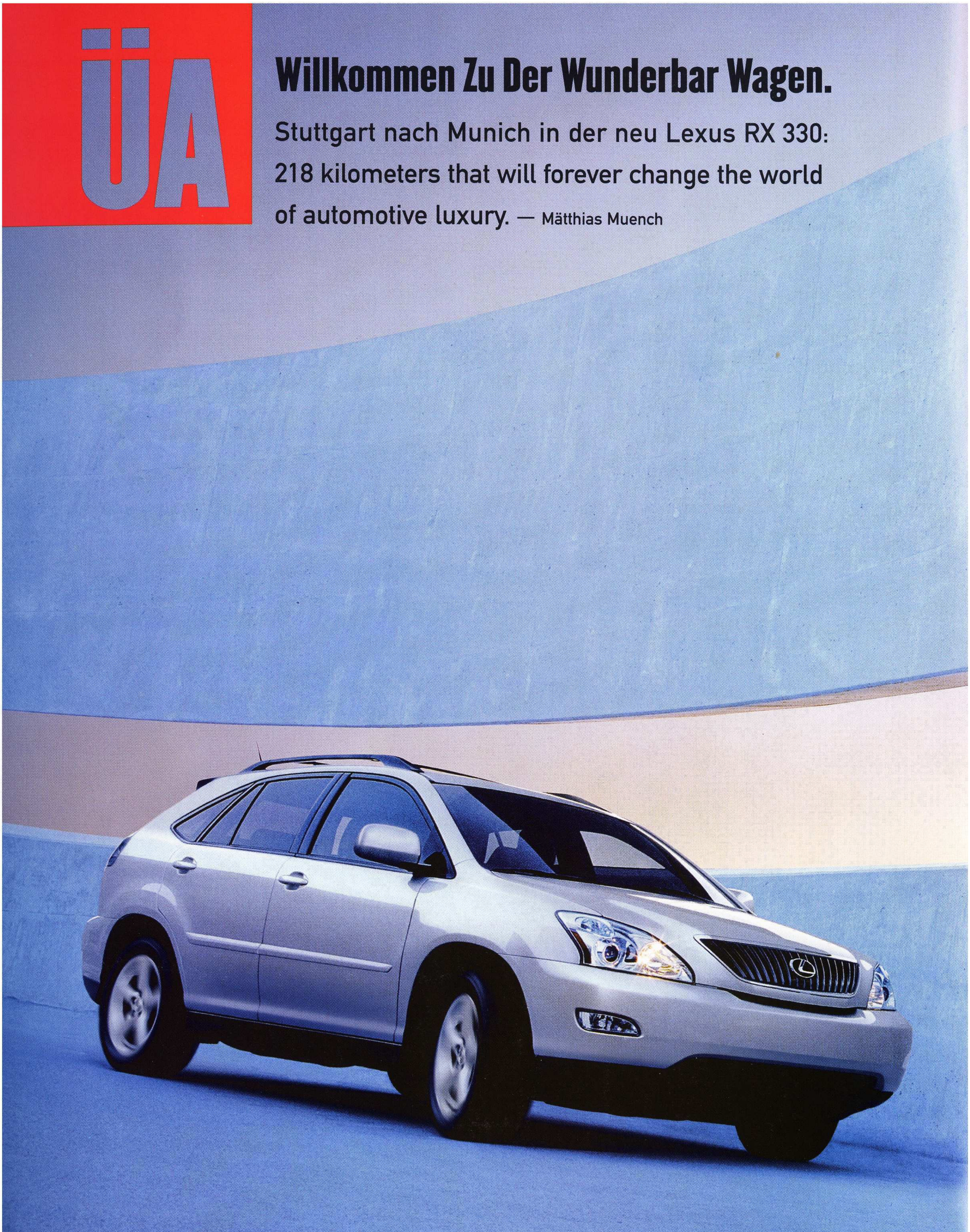
The Nano Sorter

Terrorism Information Awareness

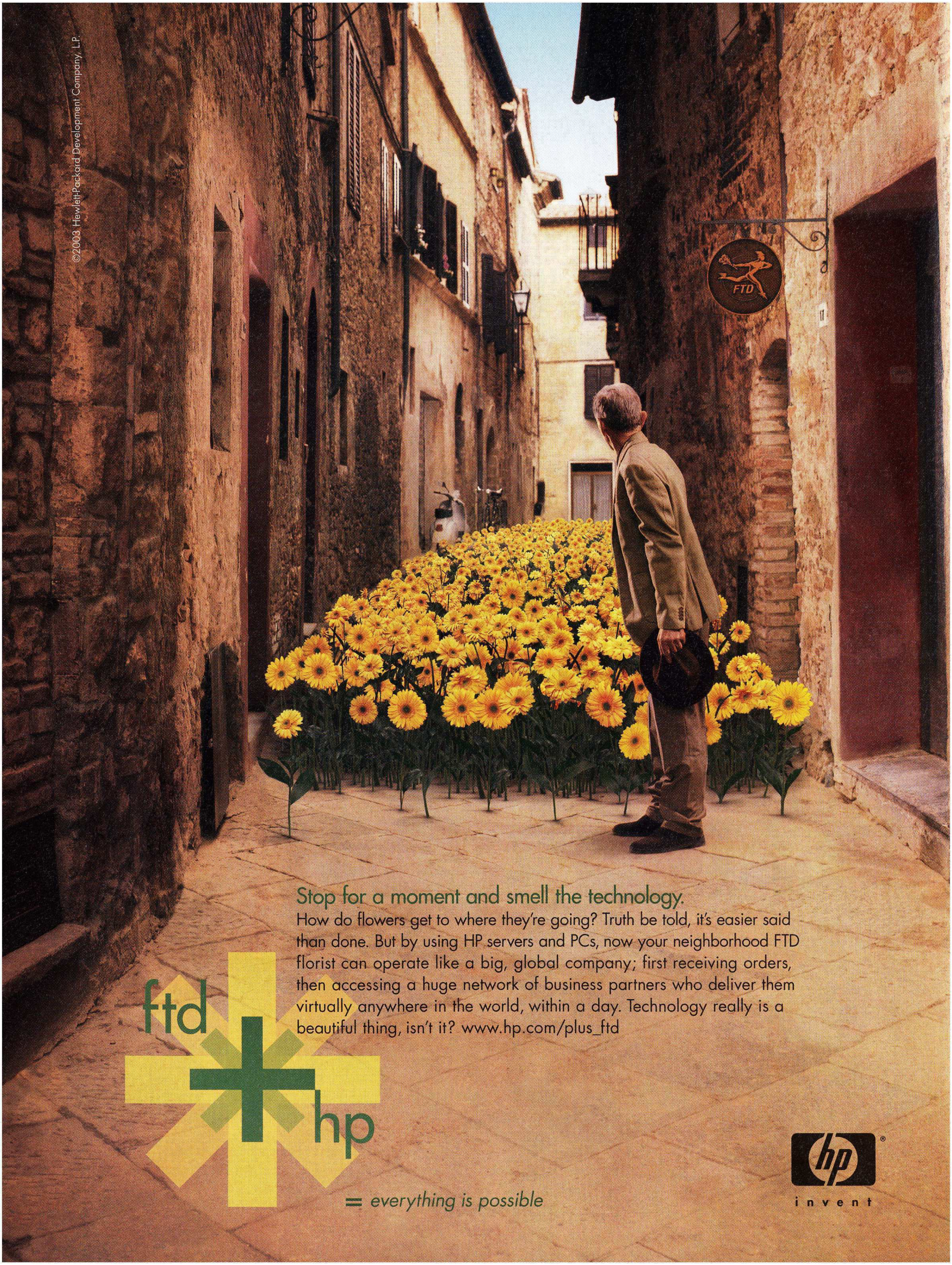
USA $4.99 • CANADA $6.99

08

0 09281 01308 2

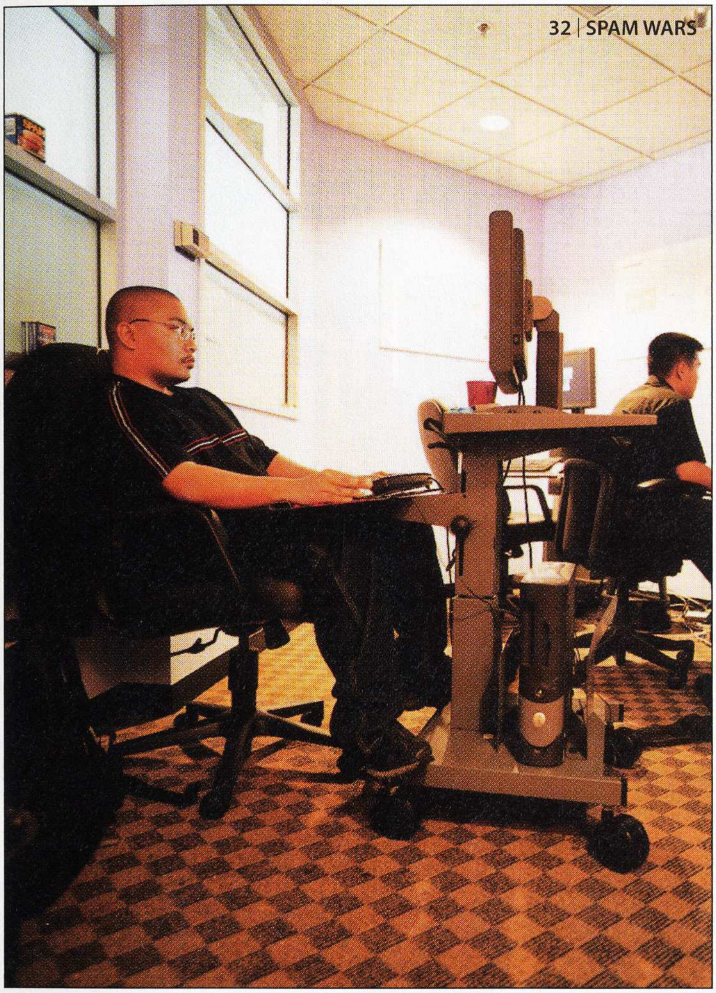

ÜA
Willkommen Zu Der Wunderbar Wagen.
Stuttgart nach Munich in der neu Lexus RX 330:
218 kilometers that will forever change the world
of automotive luxury. — Mätthias Muench

I AM A CISCO 7960G IP PHONE.


©2003 Hewlett-Packard Development Company, L.P.
FTD
Stop for a moment and smell the technology.
How do flowers get to where they're going? Truth be told, it's easier said than done. But by using HP servers and PCs, now your neighborhood FTD florist can operate like a big, global company; first receiving orders, then accessing a huge network of business partners who deliver them virtually anywhere in the world, within a day. Technology really is a beautiful thing, isn't it? www.hp.com/plus_ftd
ftd
+
hp
= everything is possible
hp
invent

CONTENTS

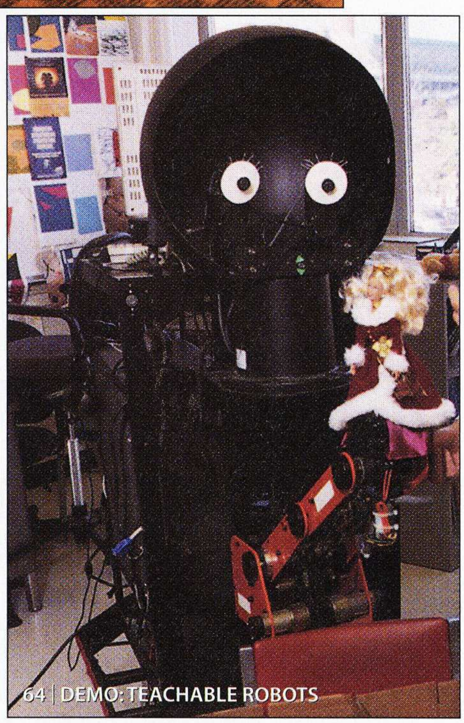
TECHNOLOGY REVIEW VOLUME 106, NUMBER 6



32 | SPAM WARS

July/August 2003

58 | SAVING LIVES WITH LIVING MACHINES



64 | DEMO: TEACHABLE ROBOTS

COVER STORY

32
Spam Wars
The proliferation of junk e-mail is threatening to overwhelm the Internet. Software companies are rushing to build defenses—but will the new technologies do more harm than good?
BY EVAN I. SCHWARTZ

FEATURES

40
Biotech's Big Chill
ESSAY | Government efforts to keep science and technology out of terrorist hands conjure images of the Cold War. But it's biomedical researchers in the United States who could be frozen out.
BY DANIEL J. KEVLES

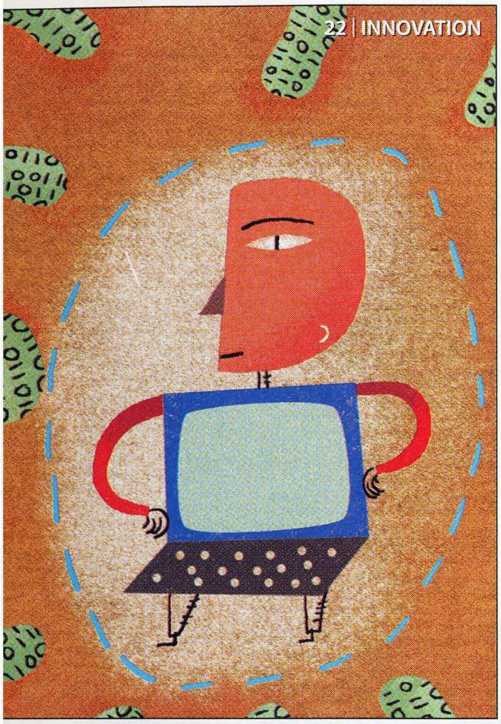
50
Casting the Wireless Sensor Net
Smart, networked sensors will soon be all around us, collectively processing vast amounts of previously unrecorded data to help run factories, maintain crops, and even watch for earthquakes.
BY GREGORY T. HUANG

58
Saving Lives with Living Machines
Hybrid devices that are part machine, part living cells, offer new hope to patients for whom purely artificial treatments like dialysis aren't good enough.
BY PETER FAIRLEY

64
Teachable Robots
DEMO | Michigan State University researcher Juyang Weng shows off his "developmental" robots, which learn the same way kids do.

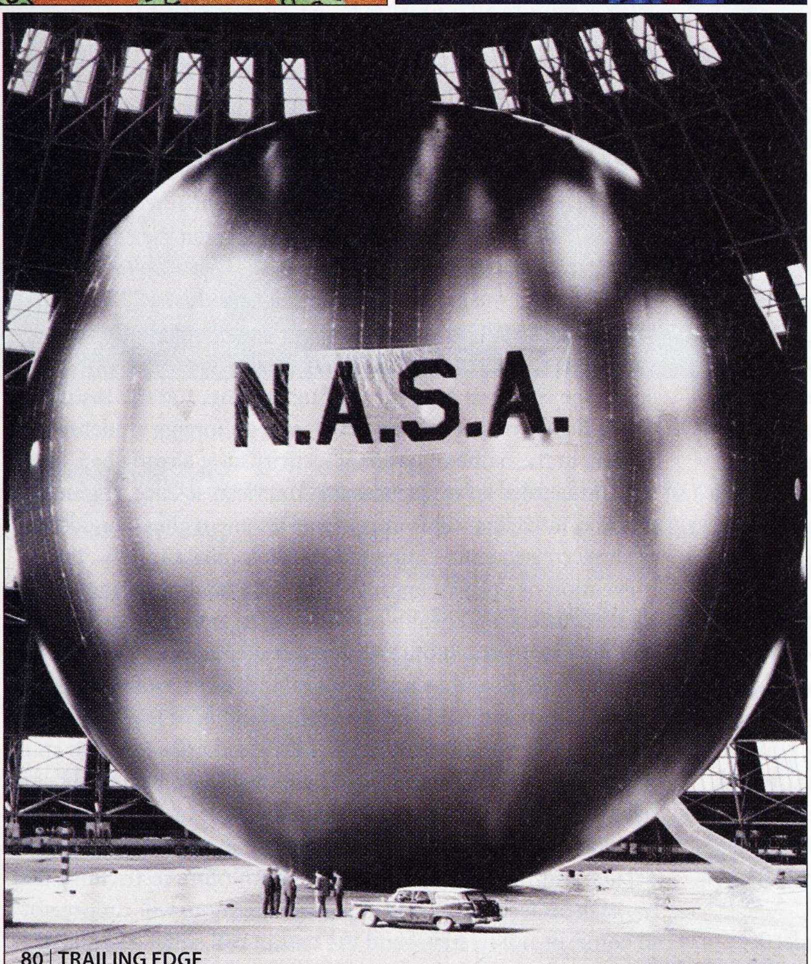

Delivering perfect sound.
Bang & Olufsen's innovations are desired all over the world—and therein lies the challenge. With HP technology powering everything from production to retail, B&O's single Denmark factory can meet demand around the globe, delivering their products as faithfully as their products deliver sight and sound. www.hp.com/plus_bang-olufsen
bang & olufsen
+
hp
= everything is possible
hp
invent
© 2003 Hewlett-Packard Development Company, L.P.

TECHNOLOGY REVIEW VOLUME 106, NUMBER 6



22 | INNOVATION

68 | POINT OF IMPACT



80 | TRAILING EDGE

DEPARTMENTS

8 Leading Edge
From the editor in chief

14 Letters
Insights and opinions from our readers

18 Prototype
Straight from the lab: technology's first draft
Mighty Micromixer ■ Marrow Measures ■ Pocket Brain ■ And more...

22 Innovation
The forefront of emerging technology, R&D, and market trends
Monitoring Mom ■ The Nano Sorter ■ Computer Immunity ■ And more...

68 Point of Impact
Where technology collides with society, business, and personal lives
Co–program manager Robert L. Popp on the U.S. Defense Department's Terrorism Information Awareness project.

73 Visualize
How 3-D ultrasound works.

78 Index
People and organizations mentioned

80 Trailing Edge
Lessons from innovations past
Satellite communication's ascent.

COLUMNS

20 Michael Schrage
Wi-Fi, Li-Fi, and Mi-Fi
Wi-Fi's future depends on whether big tech companies consider it friend or foe.

30 Simson Garfinkel
The End of End-to-End?
Internet service providers that control network content will kill innovation.

74 Seth Shulman
Thinking like a Virus
The search for SARS was a success because of global collaboration.

TECHNOLOGICAL MCCARTHYISM

Almost 50 years ago, in April of 1954, Vannevar Bush testified before a government review board in defense of J. Robert Oppenheimer. It was the heyday of McCarthyism, and Oppenheimer, an atomic-bomb pioneer, was being investigated for his opposition to the hydrogen bomb and his alleged left-wing associations. Bush, who had headed virtually all civilian military research during World War II, warned that the hearing ran the danger of "being interpreted as placing a man on trial because he held opinions, which is quite contrary to the American system." He continued, "If you want to try that case, you can try me. I have expressed strong opinions many times. They have been unpopular opinions at times. When a man is pilloried for doing that, this country is in a severe state. Excuse me, gentlemen, if I become stirred, but I am."

And excuse me if I am also stirred—by events today. Having great faith in American openness and democracy, I have always found it hard to understand how McCarthyism took hold. Certainly, during my adulthood, this country's democratic values have been periodically tested. But still I couldn't see how anything as extreme and widespread as McCarthyist ultranationalism could reappear. After reading "Biotech's Big Chill," which begins on page 40, I am no longer so certain. The story outlines how, in response to terrorism, the United States government is increasing restrictions on foreign students and limiting the access of both foreign and U.S. citizens to various materials and lines of research—mostly biological. While some of these changes are reasonable, I fear that on the whole we are coming perilously close to something similar to McCarthy's 1950s.

"Biotech's Big Chill" is written by Daniel J. Kevles, a noted Yale University historian and a contemporary observer of science and technology in society. He is also a member of the Science, Technology, and Law Panel of the National Research Council (the principal operating arm of the National Academy of Sciences and the National Academy of Engineering), which has considered some of the emerging issues in science and national security. Kevles, of course, speaks for himself alone. In his piece, he notes that during the Red Scare scientists came under scrutiny because of past or present political affiliations—and that they could theoretically be cleared of suspicion by repudiating those affiliations or any "dubious" actions. "In contrast," he writes, "what makes a scientist suspect today is his or her nationality, which is difficult to modify, or ethnicity, which is unchangeable." Such restrictions, coupled with other new rules and regulations, Kevles concludes, "may pose difficulties for contemporary biology that are far more chilling than those prevailing in early Cold War physics."

I'm not saying the government is wrong to act. Indeed, some new restrictions—namely, increased controls on biological agents such as Ebola and anthrax—are entirely prudent. But the government has also categorically excluded certain researchers, those coming from nations on its list of state sponsors of terrorism, from working with these agents. That seems both lazy—there are such things as background checks, after all—and undemocratic. And it's just the edge of the storm cloud looming on the horizon for foreign researchers in this country.

Under the latest controls, all foreign nationals from 25 countries entering the U.S. to study *anything*, not just biology, must be registered in the government's new tracking system. Anyone from this list of nations must be fingerprinted, photographed, and interviewed by the immigration service. What's more, if foreign students stay in the U.S. after graduation, they must be tracked for three years by their alma maters—which must submit regular updates to federal authorities.

Restraints on foreign students have impaired research collaborations, prevented talented scientists and engineers from entering the country, and hampered international conferences.

Kevles's article homes in on biology and biotechnology, fields in which foreigners represent a significant portion of the work force—and where the aura of restraint and caution is especially strong. In part because the new climate discourages foreign nationals from working for U.S. firms, and in part because it discourages sharing of information among colleagues, "it could," Kevles writes, "thus threaten the engineering of therapies and cures and as such place at risk the very competitiveness of the nation's biotechnology industry." But the ramifications go far beyond biotechnology. A December 2002 statement by the presidents of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine concludes that constraints on foreign students and visitors in the name of national security have already had "serious unintended consequences for American science, engineering, and medicine." This important statement cites as evidence of these consequences impaired research collaborations, the prevention or delay of approvals for "outstanding young scientists, engineers, and health researchers" to enter the country, and the hampering of international conferences.

U.S. science and technology, and indeed economic growth, have always benefited from a continual influx of talented foreigners who embrace democratic ideals and opportunities and therefore stay in the country—where they make wonderful contributions. Increasingly, these talented people have many other options in Europe and Asia. Especially if another terrorist event occurs, and we knee-jerk our way to even more restrictions that make them feel like second-class citizens, more will choose not to come, or not to stay—and the nation will suffer. I can just hear Vannevar Bush becoming stirred again. —*Robert Buderi*

MIT'S MAGAZINE OF INNOVATION
TECHNOLOGY REVIEW

EDITOR IN CHIEF
Robert Buderi

EXECUTIVE EDITOR David Rotman

DEPUTY EDITOR/WEB EDITOR Herb Brody

MANAGING EDITOR Tracy Staedter

ART DIRECTOR Eric Mongeon

SENIOR EDITORS Sally Atwood, Wade Roush, David Talbot, Rebecca Zacks

SENIOR ASSOCIATE EDITOR Erika Jonietz

ASSOCIATE EDITOR Megan Vandre

STAFF WRITER Gregory T. Huang

ASSISTANT ART DIRECTOR Jamie Kelleher

COPY CHIEF Larry Hardesty

FACT CHECKER Lisa Scanlon

PRODUCTION MANAGER Valerie V. Kiviat

EDITORIAL ASSISTANT Alyssa Danigelis

CONTRIBUTING WRITERS
Ivan Amato
Jon Cohen
Peter Fairley
David H. Freedman
Simson Garfinkel
Charles C. Mann
Michael Schrage
Evan I. Schwartz
Seth Shulman
Gary Taubes
Claire Tristram
M. Mitchell Waldrop

TR RELAUNCH FUND
MILLENNIAL PATRON
Robert M. Metcalfe
CENTENNIAL PATRONS
Steve Kirsch, DuWayne J. Peterson Jr.

CUSTOMER SERVICE/SUBSCRIPTION INQUIRIES
NATIONAL: 800-877-5230
INTERNATIONAL: 386-447-6352
www.technologyreview.com/customerservice
Cost $34 per year
Canada residents add $10
Other foreign countries add $30

PERMISSIONS
978-750-8400
www.technologyreview.com/customerservice/permissions.asp

REPRINTS
717-399-1900 ext. 118
technologyreview@reprintbuyer.com
or www.technologyreview.com/customerservice/reprints.asp

ADDRESS CHANGES
www.technologyreview.com/custserv/addresschange
MIT Records 617-253-8270 (alums only)

TECHNOLOGY REVIEW
One Main Street, 7th Floor, Cambridge MA 02142
TEL: 617-475-8000 FAX: 617-475-8043
www.technologyreview.com

MIT'S MAGAZINE OF INNOVATION

TECHNOLOGY REVIEW

PUBLISHER AND CEO
R. Bruce Journey, bruce.journey@technologyreview.com

VICE PRESIDENT AND GENERAL MANAGER
Martha Connors, martha.connors@technologyreview.com

VICE PRESIDENT, SALES AND MARKETING
Kate Dobson, kate.dobson@technologyreview.com

CORPORATE

DIRECTOR OF BUSINESS DEVELOPMENT
J. R. "Matt" Mattox
matt.mattox@technologyreview.com

DIRECTOR OF INFORMATION TECHNOLOGY
Lon Anderson

NETWORK COORDINATOR
Scott Hendry

EXECUTIVE ASSISTANT TO THE CEO
Kelli Talbot

FINANCE

CONTROLLER
John W. Keegan

SENIOR ACCOUNTANT
John F. Leahy

ACCOUNTANT
Letitia Trecartin

INTERN
Walter Rodriguez

SALES AND MARKETING

ASSISTANT TO THE VP, SALES AND MARKETING
Sharon Morani

ADVERTISING SERVICES MANAGER
Amy McLellan
amy.mclellan@technologyreview.com

SENIOR MARKETING MANAGER
Kathleen Kennedy

CONSUMER MARKETING

DIRECTOR OF CIRCULATION AND CONSUMER MARKETING
Elaine Spencer

ASSOCIATE CONSUMER MARKETING DIRECTOR
Corrine L. Callahan

DIRECT RESPONSE MANAGER
Sharon Maxwell

TECHNOLOGYREVIEW.COM

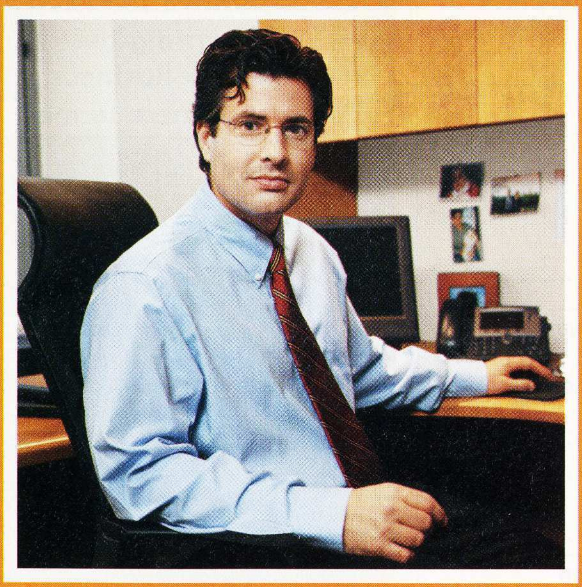
SENIOR GRAPHIC DESIGNER
Matthew Bouchard

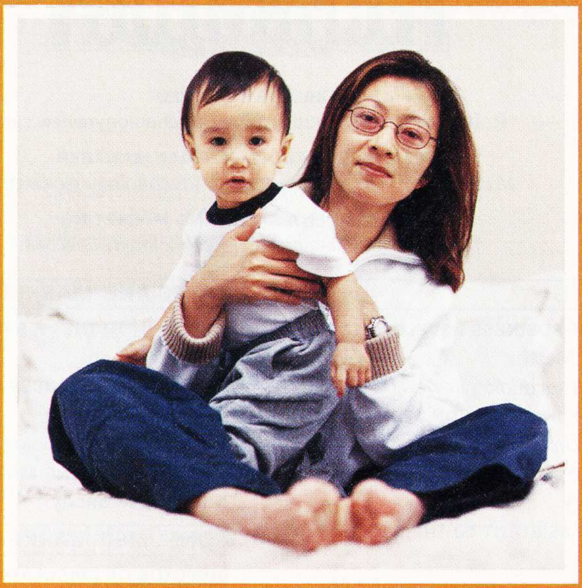
ASSOCIATE WEB PRODUCER
Thomas Pimental

CONTENT SPECIALIST
Johanna Purcell

ADVERTISING SALES

	UNITED STATES	
MICHIGAN/DETROIT: 248-546-2222	Colleen Maiorana	colleenm@maiorana-partners.com
	Sue Scott	sscott@maiorana-partners.com
MID-ATLANTIC/NEW YORK: 212-419-2820	Alan Levine	alan.levine@technologyreview.com
	Mason Wells	mason.wells@technologyreview.com
MIDWEST/CHICAGO: 312-629-5264	Chris Svoboda	amssvoboda@aol.com
NEW ENGLAND/BOSTON: 617-475-8004	Paul Gillespie	paul.gillespie@technologyreview.com
NORTHWEST/SAN FRANCISCO: 415-659-2980	Merrick Musolf	merrick.musolf@technologyreview.com
SOUTHERN CALIFORNIA/L.A.: 310-451-5655	Gregory Schipper	g@whiteassociates.com
SOUTHWEST/DALLAS: 972-625-6688	Randy Artcher	randy.artcher@tierney.com
	Steve Tierney	steve.tierney@tierney.com
	ASIA	
CHINA, HONG KONG, PHILIPPINES, AND THAILAND: 852-28-38-87-02	Herb Moskowitz	mediarep@netnavigator.com
JAPAN: 813-3261-4591	Shigeru Kobayashi	shig-koby@media-jac.co.jp
SINGAPORE: 65-98-29-90-48	Jocelyn Domingo	jdomingo@singnet.com.sg
SOUTH KOREA: 82-27-39-78-40	S. Y. Jo	biscom@unitel.co.kr
TAIWAN: 886-2-25-23-82-68	Keith Lee	leekh@ms4.hinet.net
	AUSTRALIA	
61-2-9929-5929	Anton Gruzman	sthpac@ozemail.com.au
	EUROPE	
EUROPE: 44-207-630-0978	Anthony Fitzgerald	afitzgerald@mediamedia.co.uk
	David Wright	dwright@mediamedia.co.uk
GERMANY: 49-89-5507-9909	Marcus Plantenberg	m.plantenberg@pms-plantenberg.de
	ISRAEL	
972-9-9586-245	Dan Ehrlich	d_ehrlich@netvision.net.il
	ONLINE ADVERTISING	
212-419-2824	Anne Toal	anne.toal@technologyreview.com





I run the
IT department.

I want
employees
to access
the network
without calling
me and everyone
who works for me.

I run my
household.

I want
to think
about more
important things
than phone rates,
phone bills and
phone companies.

Not available in all areas.

A NEW WAY TO LIGHT

While new LEDs are twice as efficient as incandescent bulbs, they don't come close to matching fluorescent lights ("LEDs vs. the Lightbulb," *TR* May 2003). LEDs have a potential light output of 30 lumens per watt, as compared to 10 to 15 for incandescents; but fluorescent tubes that fit into regular light sockets produce 69 lumens per watt. Although it is true that fluorescents will not challenge LEDs for traffic lights or for automobile taillights because of the harsh environments in which they operate, LEDs have a long way to go before becoming common household appliances.

Jacques Liard
Gatineau, Québec

Many of the current efforts to produce white light use phosphors to convert blue or ultraviolet light into longer wavelengths. But how well controlled is the blue itself? The day will come when municipalities consider this technology for streetlights, and it would be criminal to emit as much blue as we do now with our current technology. Besides the unpleasant glare, we would continue to condemn the night sky to invisibility.

Michael Carnes
Arlington, MA

"We should use 'smart' surveillance systems that constantly observe, but record data only when there is a noticeable change from the common pattern of behavior."

MORE COMFORTABLE SURVEILLANCE

The best way to make observations is not by recording enormous amounts of data and then processing it all the time ("Surveillance Nation—Part Two," *TR* May 2003). Instead, we should use "smart" surveillance systems that constantly observe, but go into alert mode and record data only when there is a noticeable change from the common pattern of behavior. In this case, there would be no need to record useless amounts of data, and everyone would feel comfortable—unless they were doing something wrong.

Kahren Ayrapetyan
North York, Ontario

MAKING PEER-TO-PEER PAY

The record companies just don't get it ("Curbing Peer-to-Peer Piracy," *TR* May 2003). Peer-to-peer can be excruciatingly slow, sound quality can be inconsistent due to poor encoding, the ID3s (data for identifying songs) are often wrong, and file names are not consistent. If I were in the record companies' shoes, I'd set up powerful server farms on large pipes, col-

lect reasonable monthly fees, and send out high-quality, unrestricted MP3s of every song in my entire catalogue. Give the artists a fair share of the proceeds and watch them rake in the money.

David Sewhuk
Rochester, NY

INVENTION INTERNATIONAL

As an inventor with a patent, I read Evan I. Schwartz's article ("Patents Go Global," *TR* May 2003) with interest. He discusses the issue of "first to file" versus "first to invent" as if current procedure can be easily changed. But "first to invent" is a Constitutional right, which will require an amendment to overturn. The definition of inventor includes the idea of novelty, meaning the invention was not previously known. Clearly, if an invention is previously known, the person applying for the patent is not the inventor but has merely rediscovered something already known by someone else.

Henry Baker
Encino, CA

IN DEFENSE OF REGULATORS

Michael Schrage insinuates that regulators, activists, and litigators are Luddites seeking to disrupt the introduction of new technologies without regard to their value ("Global Warning," *TR* May 2003). He also proposes that the problems of companies such as Monsanto stem from "consistently lobbing clumsy responses to public criticism." If only that were true. There are deeper reasons activists and litigators are so active. Independent science conducted by well-funded government regulators is the only ethical way to quiet activists who speak out against new technologies and processes. Such science would also go a long way toward preempting litigation. As for regulators, they are necessary in a world containing growing numbers of people and powerful technologies. The present system is suspect due to the revolving door between agencies and the industries they regulate.

Tom McGlamery
College of Engineering
University of Wisconsin-Madison

CONTACT US

E-MAIL: letters@technologyreview.com
WRITE: *Technology Review*, One Main Street, 7th Floor, Cambridge MA 02142
FAX: 617-475-8043

- Please include your address, telephone number, and e-mail address.
- Letters may be edited for both clarity and length.
- To discuss our articles online, click on Forums at www.technologyreview.com.

Corrections: In the Patent Scorecard (*TR* May 2003), the company name Magna International was misspelled. Also, Avaya is an independent company that is not owned by Lucent Technologies.

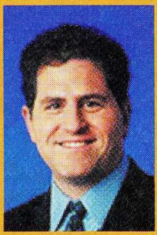
"LEDs vs. the Lightbulb" (*TR* May 2003) incorrectly implies that a typical incandescent bulb lasts about 8,000 hours. That is roughly the life of a fluorescent bulb; incandescents shine for about 1,000 hours.

Visit etc2003.com to register.

SAVE $100: Register by August 31!

The Emerging Technologies Conference at MIT

The Emerging Technologies Conference at MIT will focus on the technologies that are poised to make a dramatic impact on our world. Technology Review Magazine, the authority on emerging technology, will bring together world-renowned innovators and key leaders in technology and business. The 2-day conference will feature a mixture of keynote, panel and breakout discussions that will center on the transformative technological innovations that have the potential to fuel new economic growth.



KEYNOTE
Michael Dell, Founder and CEO,
Dell Computer Corporation

KEYNOTE
Nathan Myhrvold, Co-Founder and Managing Director,
Intellectual Ventures

KEYNOTE
Jeffrey R. Immelt, CEO and Chairman,
General Electric

TR100 HOST
Bob Metcalfe, Founder, 3Com Corporation,
Venture Partner, Polaris Venture Partners

PREMIER SPONSOR:
GMC
WE ARE PROFESSIONAL GRADE.

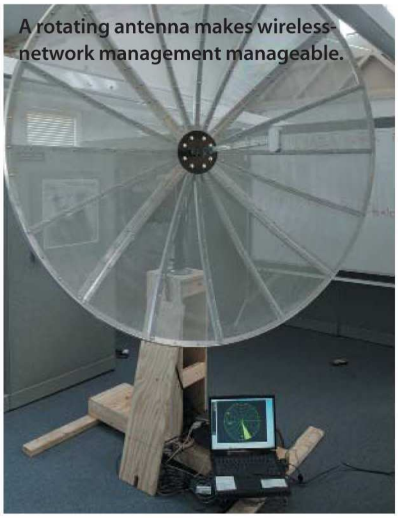
MEDIA SPONSORS:
MIT'S MAGAZINE OF INNOVATION TECHNOLOGY REVIEW
electronic design
Forbes / Wolfe NANOTECH REPORT
NANOBUSINESS alliance

PRODUCED BY:
Penton
TECHNOLOGY & LIFESTYLE MEDIA

PROTOTYPE

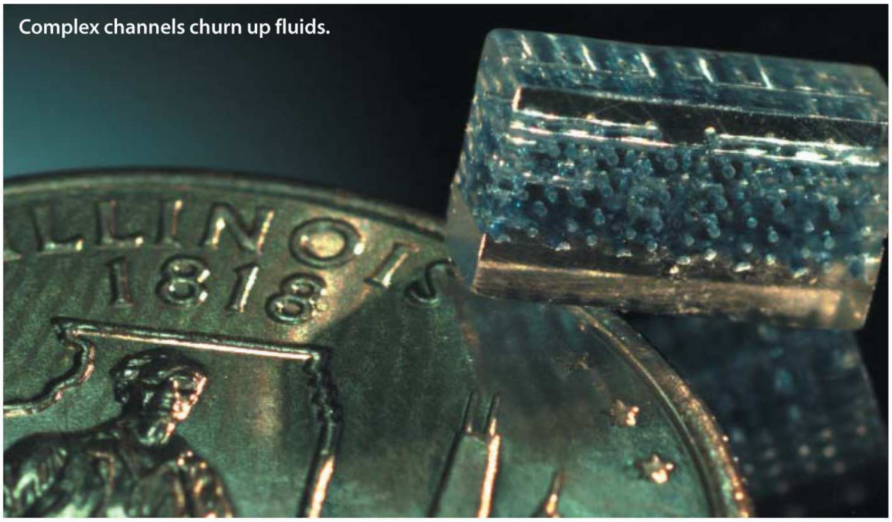
STRAIGHT FROM THE LAB: TECHNOLOGY'S FIRST DRAFT

WIRELESS MAINTENANCE



A rotating antenna makes wireless-network management manageable.

As more and more universities and companies set up wireless networks to allow untethered Web surfing, network managers are finding out what a pain it is to maintain all the equipment that keeps such systems running smoothly. Network researchers Steven Wallace and Gregory Travis of the Advanced Network Management Lab at Indiana University have come up with an automated tool that will free wireless-network operators from tedious and expensive hours of manually measuring signal strength and recalibrating transmission equipment. The system marries software to a rotating on-site antenna that periodically measures signal strength in all directions, then remotely makes any necessary adjustments to transmission devices. The Indiana researchers have already built a version of the technology able to manage small-business networks and are working on a more powerful version for university campuses and other large networks. That version will have enough range to help network administrators identify rogue users who are either monopolizing bandwidth or using the system illegally. Wallace and Travis hope to bring this technology to a mobile network near you sometime within the next year.



Complex channels churn up fluids.

MIGHTY MICROMIXER

To make medical devices that analyze tiny amounts of fluid, researchers are building biochips with increasingly complex patterns of channels. At the University of Illinois at Urbana-Champaign, materials scientist Jennifer Lewis and structural engineer Scott White have developed three-dimensional networks of channels that make fluids flow in ways that today's flat wafers can only dream of. The technology could yield chips for DNA and blood analysis able to handle more complex tasks, circulatory networks that pump chemical glues through self-healing materials, and even tiny but sophisticated chemical reactors. The new biochip's geometry—channels 10 to 300 micrometers in diameter that look like interconnected square spiral staircases—allows it to mix and process fluids in much less space than current planar chips. To fabricate the chips, a syringe dispenses 16 layers of a special "ink" in staircase patterns across a substrate layer of Teflon. The resulting structure is then coated with resin and heated; the heat melts the ink so it can be vacuumed away, leaving a network of channels that are modified to form mixing towers. The researchers have filed a patent on the technology.

MAKING DIABETES A GAME

A new wireless game could help kids with diabetes stay healthy. Many of them don't record their blood-glucose levels properly, so they don't get the right doses of insulin. To play the game, developed at Harvard University and MIT, a kid checks her glucose level with a meter that beams the data to a personal digital assistant, into which she also enters her insulin dosages. The PDA wirelessly transmits that data to a central server and, after the day's third test, redownloads its most recent records. The child then guesses what her next glucose level will be, based on the trends she notices. Lori Laffel, a pediatrician coordinating a study to test the game at Harvard's Joslin Diabetes Center, says kids playing the game check their glucose levels more often than those not playing. A larger study is planned for the end of the year, in preparation for commercializing the game.

SHOT IN THE DARK

If a gun goes off in an abandoned junkyard, does anyone hear it? The police do, at least in the handful of U.S. cities equipped with gunshot detection sensors, which listen for weapons' acoustical signatures and clock the arrival of sound waves to triangulate their origin. But these sensors must be plugged into telephone lines, meaning they can't be installed in out-of-the-way places, and a separate detector is needed every 300 to 400 meters to produce accurate results. Now New Orleans, LA-based Proxity Digital Networks is testing battery-powered detectors that can be clamped onto trees and poles and that communicate wirelessly with communications towers up to five kilometers away. The Tulsa County, OK, sheriff's department is testing the system, which transmits information on the location of gunfire to officers on patrol. It can even identify specific types of weapons, which helps police "dispatch a more effective response team specific to the situation," says Tulsa County sheriff Stanley Glanz.

Wireless sensors listen for gunfire.

COURTESY OF PROXITY DIGITAL NETWORKS (SHOT); COURTESY OF DANIEL THERRIAULT (MICROMIXER); COURTESY OF THE ADVANCED NETWORK MANAGEMENT LAB, INDIANA UNIVERSITY (WIRELESS)


A portable drill can start an IV in an emergency.

MARROW MEASURES

In more than 30 years in emergency medicine, Larry Miller saw hundreds of patients who needed intravenous fluids or drugs immediately—but didn't get them because paramedics or doctors couldn't find a suitable vein. So the CEO of San Antonio, TX-based VidaCare, along with researchers at the University of Texas Health Science Center in San Antonio, developed a device to take advantage of what World War II medics called "the noncollapsible vein": the bone marrow. After a caregiver injects a local anesthetic, the small, battery-powered drill inserts a hollow needle into the core of the shin bone, just below the knee, with the press of a button. From start to finish, hooking up a patient to fluids takes only 10 seconds or so, Miller says. Surveys show that paramedics can't start IVs for between 10 and 15 percent of patients who need them, translating to millions who could benefit from the drill each year. Miller expects U.S. Food and Drug Administration approval for the device by the end of the summer.

TACTICAL TUTOR

You're a tank commander in the U.S. Army. As your battalion approaches a bridge, you see that it's in enemy hands. Do you retreat, engage the enemy, or try to stop the flow of enemy troops crossing the river? That's a scenario posed by training software being developed by San Mateo, CA-based Stottler Henke. The software mimics a human tutor, examining the decisions a trainee makes on a simulated battlefield. Unlike existing training programs, the system uses artificial intelligence to interact with the trainee in dialogues where there isn't one correct course of action. It also adapts to the user's individual strengths and weaknesses, coming up with questions based on his or her battle plan. Currently, the interface is a keyboard and screen with maps and text, but programmers may design a new speech interface. Initial versions of the software will be ready for use by the army within a year, says Eric Domeshek, the project's manager. Commercial applications abound, he adds—such as e-tutors for teaching marketing strategy in business schools.


Infrared light spots hamburger contamination.

MEAT MONITOR

So far, mad-cow disease hasn't been detected on U.S. soil, but food safety experts are still keen to ensure that the burgers on the grill this summer don't carry the proteins that cause the disease. A test developed at the University of Arkansas could help. It uses conventional infrared spectroscopy to examine ground meat for contamination with tissue from the central nervous system; such tissue is thought to carry the proteins and is forbidden in meats by the U.S. Department of Agriculture. The process, which could be integrated into meat production lines, is more sensitive than current methods, which sample only small amounts of meat using biological assays to find central-nervous-system proteins. Of particular concern, says Arkansas animal scientist and system coinventor Fred Pohlman, are automated meat recovery systems, which strip muscle from beef bones—including the spine. In a 2002 survey, about 35 percent of meat produced by such systems was contaminated. Pohlman believes that with further development, the infrared scan could turn a potential burger nightmare back into a summer dream.

POCKET BRAIN

A computer's keyboard and screen are merely for interacting with its real guts: processor and memory. So why lug these interfaces around every time you want to take your computer across the hall? You won't have to, if the "Personal Server" project led by computer scientist Roy Want at Intel Research in Santa Clara, CA, succeeds. Want's team's prototype—roughly the size and weight of a deck of cards—has a 200-megahertz processor, a one-gigabyte flash memory card, a rechargeable battery, and a radio transceiver. Put it next to any computer equipped with a wireless card and special software, and the miniserver shows up on the desktop as a separate drive. The project grew out of recent advances in processor efficiency, memory capacity, and wireless transmission speeds, says Want. "We've just crossed the threshold. Music, videos, text files—now you can put all of those things in your top pocket." Intel will commercialize the device once prices for the components hit a "sweet spot," says Want—which could happen within a year.


Pack your files onto a pocket-sized server.

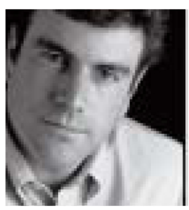
COURTESY OF ROY WANT, INTEL (POCKET BRAIN); COURTESY OF THE UNIVERSITY OF ARKANSAS (MEAT MONITOR); COURTESY OF VIDACARE (MARROW)

WI-FI, LI-FI, AND MI-FI

In any analysis of innovation, 802.11 is truly a prime number. This evolving standard, better known as Wi-Fi, is the "it" protocol that's won the same spectacular hype as (whisper it softly) the Internet itself. Oh, the good old days. I miss them.

But while Wi-Fi undeniably inspires that intoxicating blend of expectation and excitement that leads to entrepreneurial excess, it's also the kind of technological platform that invites the best ideas. Wi-Fi's combination of well-crafted technical standard and regulation-free deployment offers a robust model for digital development. Alas, whether this model is ultimately sustainable for *marketplace* development remains an open question. After all, the ongoing explosion of network innovations has hardly improved the financial health of the telecom industry.

Which is why Wi-Fi makes such an interesting case study in the economics of innovation adoption. For example: does the rise of Wi-Fi make telephone companies' underutilized fiber backbones more valuable or less valuable?



That's a multibillion-dollar question in the United States alone. Who knows? I don't. But it's not a bad bet that by increasing the number of settings where people can use their computers, ubiquitous Wi-Fi will dramatically increase bandwidth demand rather than radically reduce it.

That would surely give the telecom industry powerful economic incentives to treat Wi-Fi as a potential "force multiplier" for its networks rather than a threat. Perhaps that's why Bell Canada, Verizon, and other phone companies say they intend to turn their cell-obsoleted pay phones into Wi-Fi access points.

Then again, to the extent that Wi-Fi capabilities supersede—rather than complement—cellular, fiber, and copper nets, the technology subverts existing telecom business models. So should these companies embrace Wi-Fi or strangle it? An old political adage comes to mind: "Keep your friends close and your enemies closer."

But let's consider a bold rival approach to promoting Wi-Fi. This idea builds upon the open-source ideology of shared development and distribution, as well as "viral marketing," which turns customers into resellers. The concept is to create a Wi-Fi cooperative that turns individual laptops into potential nodes, routers, and hubs of a global network analogous to the wireless-mesh networks being pursued by Intel, among others.

So treat every laptop as a voluntary Wi-Fi hot spot. People could go online to retrieve software that effectively turns their machines into Wi-Fi access points. Instead of paying for broadband Internet subscriptions, individuals—and organizations—would agree to make their machines accessible to other machines, creating relays that eventually reach the Net. In the same way that individuals and institutions license their "free" access to open-source Linux, they would have "free" access to their open-source Wi-Fi.

In acknowledgement of Linux, let's call this approach Li-Fi. The more people who participate, the greater the number of access points and the denser and richer the networks. In the same way that Linux threatens Microsoft, Li-Fi could threaten traditional networking and telecom.

But wait! How about Microsoft building this capability into its operating systems? In exchange for agreeing to turn your laptop into a shared hot spot/access point, Microsoft will give you free or discounted upgrades of its software. Bang—with its desktop/laptop dominance, Microsoft is now the biggest player in data networking. Call this approach "Mi-Fi." (Bill, feel free to call me about this.)

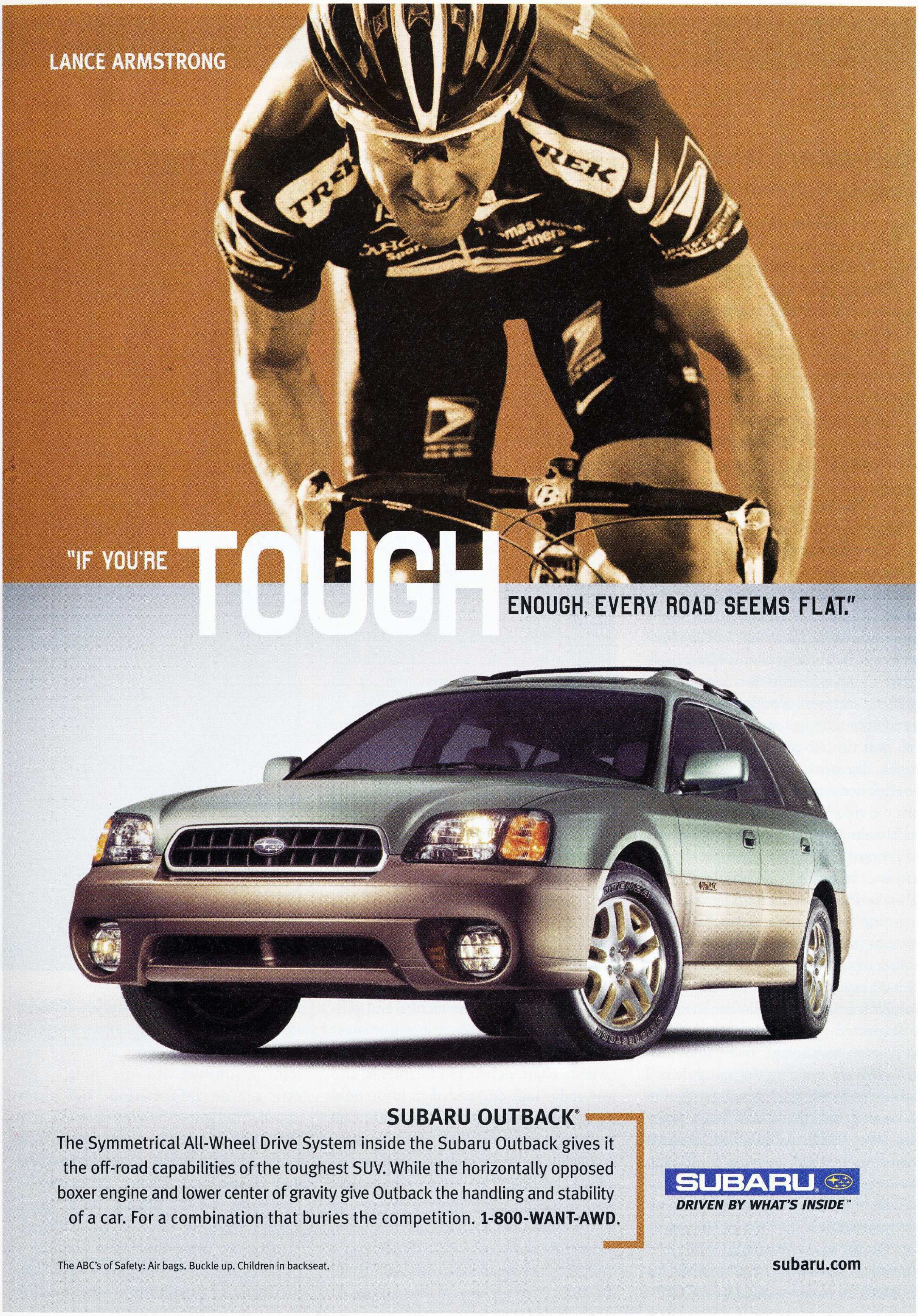
To be sure, just as there's no such thing as a free lunch, there's no such thing as a free innovation. Wi-Fi, however,

How about Microsoft building Wi-Fi into its operating systems? You make your laptop an access point, and Microsoft gives you free upgrades. Call it "Mi-Fi." (Bill, feel free to call me about this.)

comes appealingly close. Wi-Fi hot spots where passersby can piggyback, by invitation or not, on someone else's wireless network are already "war chalked" on the sidewalks of New York and San Francisco. Philanthropies have endowed "free" Wi-Fi access in parts of Manhattan and other metropolitan areas. Wouldn't it be interesting if the increasing number of public-private partnerships that oversee public libraries, public parks, and other public spaces offered subsidized access?

The purpose of these proposals is to remind innovators that in the end, Wi-Fi's future will be determined less by its internal technological evolution than by the ways institutions and individuals are encouraged to adopt it. Increased density will in turn inspire innovative devices. Wi-Fi/Li-Fi/Mi-Fi-enabled pay phones are too obvious; I like the idea of 802.11-powered alarm boxes, fire hydrants, videocams, and baby carriages.

Perhaps Wi-Fi, Li-Fi, and Mi-Fi promote a more cooperative economics of adoption—just as we saw with the TCP/IP protocol behind the Internet and the hypertext transfer protocol that powers the World Wide Web. That's enormously exciting, even if it isn't necessarily great business. Then again, just as the rise of Linux forces Microsoft to become more innovative, the rise of Li-Fi/Mi-Fi couldn't help but drive greater Wi-Fi innovation. That's the surest way to promote ubiquitous adoption. TR


LANCE ARMSTRONG
"IF YOU'RE TOUGH ENOUGH, EVERY ROAD SEEMS FLAT."
SUBARU OUTBACK®
The Symmetrical All-Wheel Drive System inside the Subaru Outback gives it the off-road capabilities of the toughest SUV. While the horizontally opposed boxer engine and lower center of gravity give Outback the handling and stability of a car. For a combination that buries the competition. 1-800-WANT-AWD.
SUBARU
DRIVEN BY WHAT'S INSIDE™
The ABC's of Safety: Air bags. Buckle up. Children in backseat.
subaru.com

MONITORING MOM

As population matures, so do assisted-living technologies

Eric Dishman is making a cup of tea—and his kitchen knows it. At Intel's Proactive Health Research lab in Hillsboro, OR, tiny sensors monitor the researcher's every move. Radio frequency identification tags and magnetic sensors discreetly affixed to mugs, a tea jar, and a kettle, plus switches that tell when cabinet doors are open or closed, track each tea-making step. A nearby computer makes sense of these signals; if Dishman pauses for too long, video clips on a television prompt him with what to do next.

It's all part of a growing effort at Intel and other labs around the country to develop ways to help the elderly, and others who need assistance with everyday activities. Similar systems are in the works to monitor eating, sleeping, and medication habits in order to allow older people to live independently for longer. Researchers are even working on systems that analyze changes in behavioral patterns over time to provide early warning of aging diseases such as Alzheimer's.

High-tech systems to monitor and assist the elderly are now becoming practical, thanks to the falling prices of sensors and processors, increasingly sophisticated software, and the wide availability of high-speed Internet access. They are also becoming increasingly attractive as a business; in the United States alone, the number of people over age 65 is expected to hit 70 million by 2030, doubling from 35 million in 2000, and similar increases are expected worldwide. "You've got many large technology companies like Intel suddenly noticing the aging demographics and asking, 'How will our future products fit into this space?'" says Dishman, who heads an Intel-led research consortium formed last year to develop monitoring technologies.

One of the simplest, nearer-term systems is under development by Honeywell Laboratories in Minneapolis, MN. The company is testing a home monitor for the elderly in seven assisted-living facilities in Minnesota and four homes in Florida. The Honeywell system starts with cheap, unobtrusive sensors set up around the home. Four to six motion detectors on the walls, plus a switch that detects when a pillbox is opened, are wired to a communications box in a closet which sends sensor information over the Internet to a processing station. There, software being developed by Honeywell compares what's going on in the home—when a person gets out of bed, goes to the bathroom, and so forth—to patterns recorded during a calibration period.

The goal of the software is to glean a picture of the person's daily activities. Motion in the bathroom and the opening of a pillbox, for example, would tell the computer that the person is taking medication. Activity in the kitchen would indicate the person is eating or drinking. Lack of these signals at certain times, or decreased activity overall, would suggest something is wrong; the computer would then make a telephone call with a simple reminder such as "take your pills." The system could also alert caregivers, via either a call or an e-mail. Honeywell expects to sell the system in three to five years; while the prototype costs $5,000, the commercial version should cost less than $500, says Tom Plocher, the project's leader.

The Intel consortium is developing even more sensitive ways to follow the activities of elderly people. Its research goes beyond motion detectors and pillbox sensors to include things like pressure sensors on an Alzheimer's patient's favorite chair, networks of cameras, and tiny radio tags embedded in household items and clothing that communicate with tag readers in floor mats, shelves, and walls. From the pattern of these signals, a computer can deduce what a person is doing and intervene—giving instructions over a networked television or bedside radio, or wirelessly alerting a caregiver. Dishman says Intel will install the first trial systems in the homes of two dozen Alzheimer's patients by early next year.

Crucial to the most advanced systems is software. It's one thing to get raw sensor information, but quite another to figure out what the person in the home is actually doing, says Misha Pavel, a biomedical engineer at the Oregon Health and Science University in Portland, OR. Working with Intel, Pavel's team is developing artificial-intelligence algorithms that deduce a person's intent by building a statistical hierarchy of possibilities—say, making

ANNIE MARIE MUSSELMAN

A radio frequency identification tag on an ordinary dinner plate is part of an Intel system designed to help loved ones track whether an elderly person is eating.

SAMPLING OF COMPANIES IN ELDERLY HOME-MONITORING

COMPANY	TECHNOLOGY
GE Industrial Systems (Plainville, CT)	Low-cost wireless sensing system that caregivers can access
Honeywell Laboratories (Minneapolis, MN)	Motion sensors and software that learns daily patterns of behavior in homes
Intel Research (Hillsboro, OR)	Radio chips that track activity and software that detects cognitive decline
Matsushita Electric Works (Osaka, Japan)	Interactive robot pets and advanced sensors to assist elderly nursing-home patients
Motorola's iDEN Subscriber Group (Plantation, FL)	Smart cell phones that give reminders or directions and relay vital signs to caregivers

tea, cooking, or doing dishes—that is based on past experience.

Longer term, software could even help detect disease. At the University of Rochester's Center for Future Health, researchers are using networks of video cameras and powerful computers to detect changes in behavior and coordination signaling early-stage neurological disorders. In theory, a home system might detect the onset of Alzheimer's or Parkinson's disease before a patient deteriorates enough to seek a doctor's help, says Philippe Fauchet, the center's director.

One possible sign of early-stage Alzheimer's that a monitoring system could detect: a person standing in the kitchen for a few minutes without doing anything. And to spot early Parkinson's symptoms, the Rochester researchers are developing machine vision algorithms to extract the movements of a person's arms, legs, and torso from video shot from multiple cameras in a room. This is the first step toward a software product that can detect very early Parkinson's symptoms like decreased stride length and asymmetries in arm swinging. But turning these algorithms into practical systems will take time; Fauchet predicts commercialization will take a decade.

Health-care experts foresee no shortage of customers. Larry Minnix, president of the Washington, DC-based American Association of Homes and Services for the Aging, which represents 5,600 nursing homes and elder-care facilities, says consumers will pay handsomely for technologies that keep them or their aging parents independent, alleviate caregiver burnout, and improve nursing-home care. "Good care is expensive, but inadequate care is a lot more expensive," he says. Big technology companies are betting he's right, as they bankroll these systems' transition from lab curiosities to demonstration models. "Two years from now, you will see many more trials of holistic home monitoring systems than exist today," says Dishman. After all, these technologies are about improving the lives of the elderly—and developing new markets. Neither idea is likely to get old. —*Gregory T. Huang*

Rooftop-mounted lasers send broadband data through the air.

THE LAST LASER MILE

TELECOM | **While the telecommunications industry still faces dark days, one technology can see light at the end of the tunnel. Called free-space optics, it uses window- or roof-mounted lasers to transmit data from main fiber-optic lines through the air to end users. When the technology was commercially introduced several years ago, only a few corporate clients signed on, seeking faster service in large office buildings. Big telecom carriers stayed away, convinced they had the capital to dig up streets and sidewalks to bring more-reliable, but far more expensive, optical fiber to millions of individual customers.**

But bad times killed most of those plans, giving a boost to free-space optics as an affordable solution. In March, Terabeam in Seattle signed a deal with a Chinese telecom carrier, China Railcom, to provide free-space optical links to businesses in Shanghai. Free-space players LightPointe in San Diego and fSONA in Richmond, British Columbia, say they have similar deals in the works. Indeed, though they won't discuss current negotiations, companies such as AT&T, Verizon, France Telecom, and Bell South have all recently completed trials of the systems.

The attraction? Despite susceptibility to fog and the need for direct lines of sight, free-space links are cheap and can, unlike other wireless approaches, provide fiberlike bandwidth. Free-space companies "will be able to sell to some carriers," says Lindsay Schroth, a broadband access analyst at Yankee Group, a Boston technology consultancy. Such modest predictions are a far cry from the hubris common just a few years ago in the optical-communications industry, but at least some carriers are starting to see the light. —*Erika Jonietz*

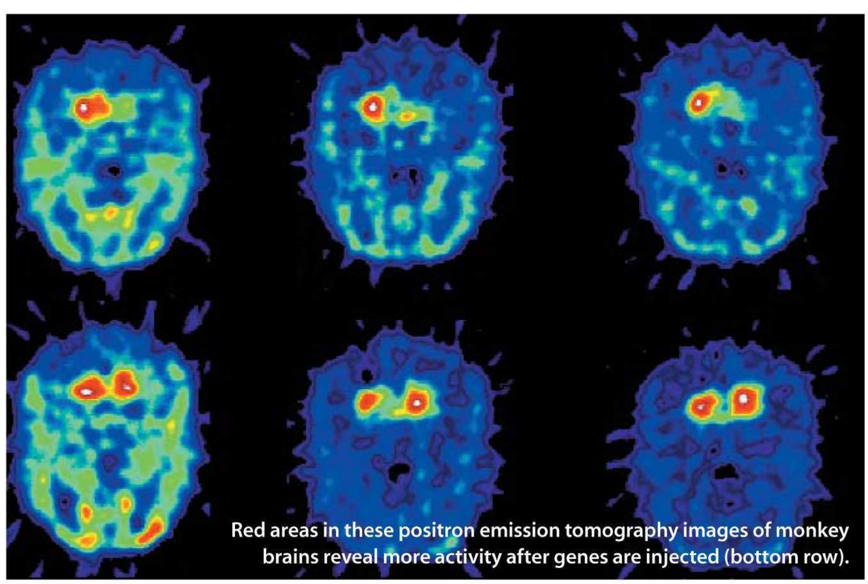
GENE THERAPY ADVANCES ON PARKINSON'S

BIOTECH | Patients with Parkinson's disease often do well for years by taking levodopa—a drug their brain cells turn into dopamine, the neurotransmitter whose decline causes debilitating spasmodic movements. Eventually, though, the drug loses effectiveness, as the patient's brain stops converting it, and symptoms worsen. But gene therapy—in which therapeutic genes supplement or replace missing or damaged ones—may keep the drug working much longer, offering hope that the lives of many Parkinson's patients can be dramatically improved.

Biologists at the University of California, San Francisco, have injected viruses carrying an enzyme-producing gene, called AADC, into monkeys' brains. The enzyme transforms levodopa into dopamine and could keep the drug working in late-stage Parkinson's patients. Krys Bankiewicz, the UCSF gene therapist who is leading the study, says levodopa still controls the symptoms of test monkeys suffering from a severe, chemically induced form of Parkinson's three and a half years after gene transfer. "There are no adverse effects that we can detect, and it's efficacious," he says. Indeed, Bankiewicz is cautiously optimistic that a very small human trial, which would also require injections into the brain, could begin as early as the end of the year.

While this approach could help patients with advanced Parkinson's, the long-term goal is to slow or halt the disease's early progression. A different gene, called GDNF, could help by protecting and perhaps regenerating dopamine-producing neurons. While much work is still needed—for one thing, the researchers must find a way to effectively turn the gene on and off—Jeffrey H. Kordower, director of the Research Center for Brain Repair at Rush Presbyterian Medical Center in Chicago, hopes that clinical trials could take place within three years.

As a means of tackling Parkinson's, gene therapy is gaining momentum. In February, a consortium of scientists at seven research centers—organized by University of Rochester neuroscientist Howard Federoff and including Bankiewicz and Kordower—received $8.8 million in federal funding to pursue gene therapy for Parkinson's. Richard Mulligan, a gene transfer expert at Harvard Medical School, says questions remain—including which gene is best—but that some form of gene therapy could very well prove effective as a Parkinson's treatment. "It's really an excellent disease target for gene therapy," he says, because the therapeutic genes need to be delivered to a specific location in the brain, which is difficult for other therapeutics to reach. If the consortium is successful, it will be a victory for both the field of gene therapy and millions of Parkinson's patients. —*Erika Jonietz*

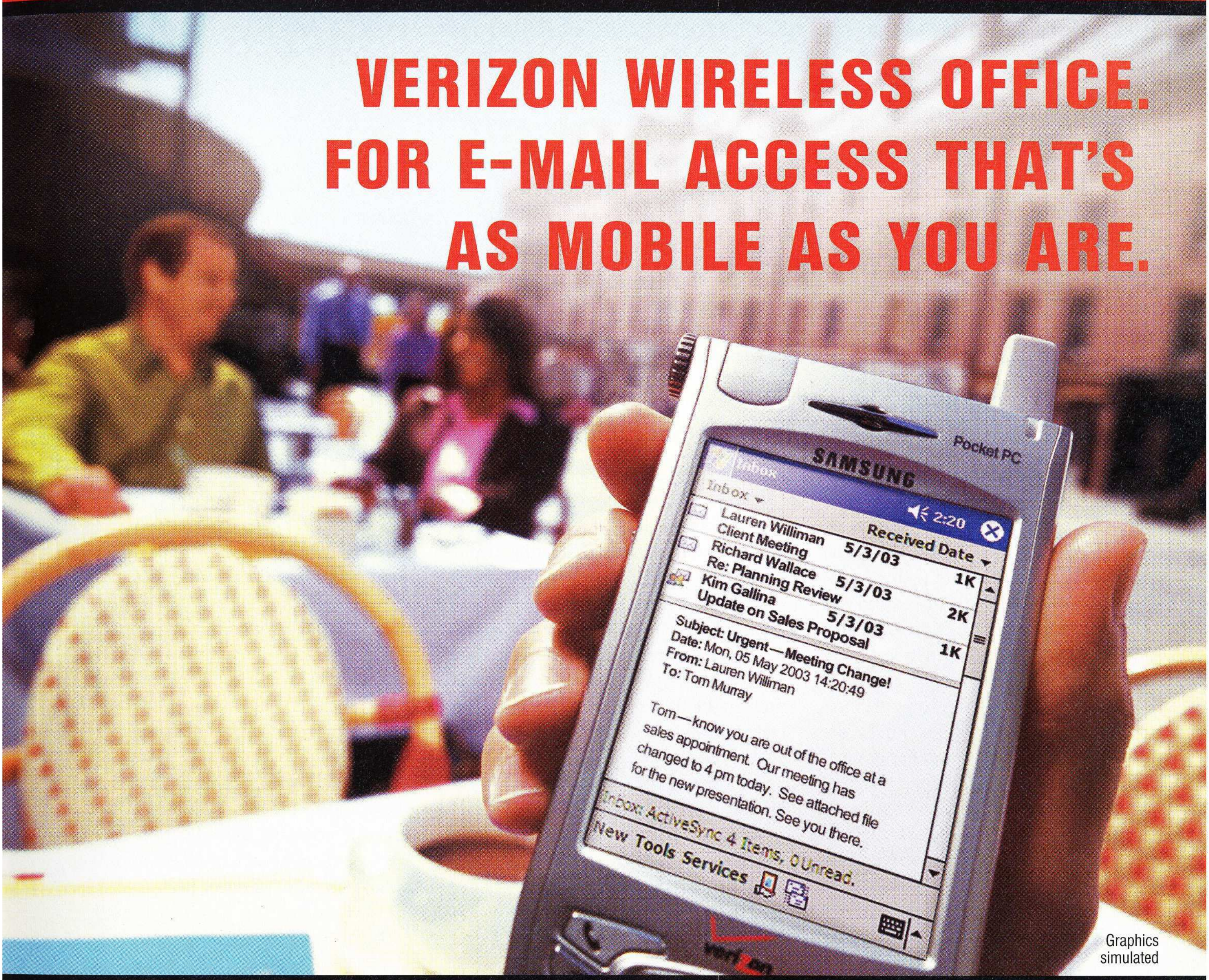


Red areas in these positron emission tomography images of monkey brains reveal more activity after genes are injected (bottom row).

COURTESY OF UNIVERSITY OF CALIFORNIA (PARKINSON'S); COURTESY OF FSONA (LASER)

VOICE TOOLS | REMOTE ACCESS | OFFICE E-MAIL & ORGANIZER | CUSTOM SOLUTIONS

VERIZON WIRELESS OFFICE. FOR E-MAIL ACCESS THAT'S AS MOBILE AS YOU ARE.

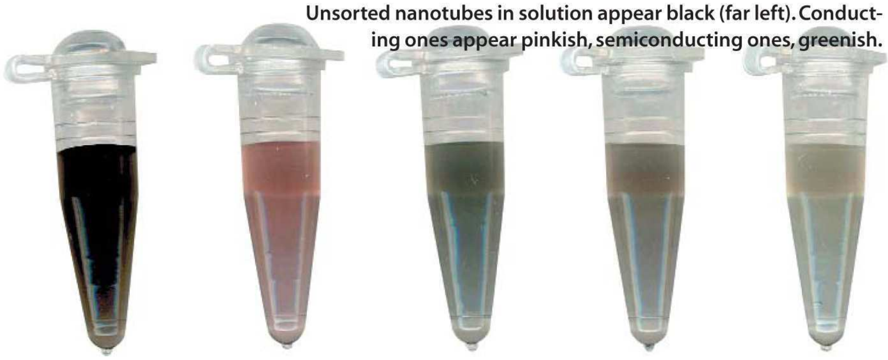


OFFICE E-MAIL & ORGANIZER from Verizon Wireless Office keeps your workforce connected to important e-mail and schedules, when they're on the go. With the latest PDAs and Smartphones from Verizon Wireless, coupled with Verizon Wireless Sync, your data travels on America's most reliable wireless network. So business outside the office becomes more productive, efficient and convenient.

Drive responsibly. Call with care.

Contact our business representatives at **1.866.899.2862** or log on to **verizonwireless.com**

verizonwireless
We never stop working for you.®



Unsorted nanotubes in solution appear black (far left). Conducting ones appear pinkish, semiconducting ones, greenish.

THE NANO SORTER

DuPont uses DNA to sort carbon nanotubes by conductivity

NANOTECH | You think it's hard keeping your tube socks organized? Try sorting carbon nanotubes, those remarkable molecules whose electrical properties make them potential building blocks for everything from ultrasensitive diagnostic devices to transistors 100 times smaller than those in today's fastest microchips. Trouble is, when nanotubes are fabricated, they're a mixed bag; some are electricity conductors, while others are semiconductors. Since a number of practical electronics applications demand nanotubes of uniform conductivity, sorting technologies are needed.

Researchers at DuPont in Wilmington, DE, say they're beginning to solve the problem using another remarkable molecule: DNA. The results are literally visible. A pink-colored vial of nanotubes in solution contains highly conducting nanotubes; other vials, with greenish hues, hold semiconducting ones. "One of the central goals of the field at the moment is to separate nanotubes, because there are applications where having mixtures of semiconducting and metal versions is a real hindrance," says R. Bruce Weisman, a chemist and nanotube researcher at Rice University. "If they've got vials of separated nanotubes, that is a big result."

The DuPont researchers found that single-stranded DNA tends to wrap around the nanotubes, forming a stable structure. To enlist this property to sort nanotubes, they engineered DNA to selectively attach to nanotubes with specific conductivities. Then they used standard lab techniques to separate the DNA-nanotube hybrids according to the natural charge of the DNA, which is different for different sequences. The attached nanotubes go along for the ride.

The company has several goals in mind, says Tim Gierke, a chemist at DuPont, which published the results in the journal *Nature Materials*. First, the researchers plan within a year or so to use DNA-nanotube hybrids in prototype sensors for medical diagnostics. For this application, they would marry nanotubes with DNA sequences that bind to complementary sequences of a pathogen's DNA; the nanotube would register the binding electrically. Longer term, sorted nanotubes—after being heated to unravel the DNA-nanotube hybrid—could be used as switches or other elements in molecular electronic devices. DuPont might even find itself becoming a supplier of custom batches of nanotubes. "We haven't sorted out just exactly how we want to consider that business opportunity," Gierke says. But at least the nanotubes themselves are now beginning to get sorted. —*David Talbot*

HELP FOR HANDHELDS

INTERFACES | **The common desktop interface of personal computing—clicking links, file names, and tabs to navigate everything from the Web to Microsoft Word—works fine on your PC but not on the tiny screens of handheld devices, which rely on cumbersome adaptations like drop-down menus and scrolling. Now, the first interface that completely replaces these methods with the simpler method of zooming—alternating levels of magnification—is headed to the handheld market.**

Users initially see a bird's-eye view of icons or text blocks representing basic information categories. They click to get a closer view and more information and pan between categories, without needing tools like the "back" button or drop-down menus, says Maximilian Riesenhuber, chief science officer of GeoPhoenix of Cambridge, MA, which is bringing the product, called Zoominator, to market this summer. The GeoPhoenix move follows a zooming trend. Already familiar in common tools like Web-based maps, zooming is showing up in more applications. For example, Windsor Interfaces of University Park, MD, a startup founded by University of Maryland computer scientist Ben Bederson, plans to market a photo browser that allows users to pan across, and zoom in on, hundreds of thumbnail images, even if they are located in different folders. As a result, users won't have to remember individual photos' names; they will be able to identify them quickly by looking at their thumbnails.

As more people use handhelds or tablet PCs instead of laptops—and styluses instead of keyboards—zooming will speed into the marketplace, says Ken Perlin, a computer scientist at New York University. "Zooming interfaces are physical and direct," he says. Riesenhuber says his goal is not only to present information in an intuitive way, but "most importantly, that you can access it from any kind of device." Long term, that might make it zoom to deskbound PCs, too. —*Megan Vandre*

JAMES YANG (ILLUSTRATION); COURTESY OF DUPONT (NANO SORTER)


Lotus. software
See who's online in real-time.
See knowledge shared in real-time.
See real-time teamwork at work.
Can you see it?
5
KEEP DRY
Lotus Instant Messaging is the leader in instant messaging for business. Lotus software lets you know who's available, on demand. It creates real-time, virtual collaboration, on demand. It can create cost savings and quicker response time instantly. Everyone becomes more agile. Your communication is more secure. Business advantage is immediate. For a Lotus webcast, visit ibm.com/lotus/seeit
e business on demand software
IBM
IBM, Lotus, the e-business logo and e-business on demand are registered trademarks or trademarks of International Business Machines Corporation in the United States and/or other countries. Certain information contained within this advertisement is based on results from the Osterman Study "Survey on Instant Messaging Issues" (9/02), which indicates that Lotus Instant Messaging is the leading solution in situations where an enterprise has settled on an IM standard. ©2002 Osterman Research, Inc.
©2003 IBM Corporation. All rights reserved.

COMPUTER IMMUNITY

Better anti-hacking tools attack invaders

SOFTWARE | For years computer scientists have dreamed of building computer security software as effective and versatile as the human immune system, which can swiftly overwhelm even intruders it has never seen before. Such a software tool would free programmers from having to anticipate and respond to the changing array of attacks hackers use; instead, it would simply allow a computer to understand its own normal behavior and shut down deviant processes.

Now such systems are finally going commercial. An intrusion prevention system from Sana Security of San Mateo, CA, is protecting private customer data for companies like Smith and Hawken, a catalogue and Internet retailer in Marin County, CA. Smith and Hawken officials say none of the many attempts to infiltrate their computers have succeeded since they began a trial run of Sana's software in mid-2002, and that hands-on monitoring has been reduced by dozens of hours a week. "I've heard the immune system analogy before in the security business, and usually my eyes roll up in my head," says Eric Ogren, a senior analyst and computer security specialist at Boston technology consultancy the Yankee Group. "What makes Sana unique is the way their software is able to automatically learn."

In the body, immune cells learn to recognize invaders by assuming that unfamiliar patterns on the surfaces of cells are foreign. Sana's software, launched commercially in March, uses a similar trick. It learns a computer's typical pattern of "system calls," or requests that a program issues to the operating system in order to carry out actions such as reading or writing on a disk. "When someone is using a flaw in a program to gain access to a system, they are typically forcing the system to do something unusual," says Sana founder and chief scientist Steven Hofmeyr. "Our 'self' is really the sequence of normal system calls, and 'nonself' is those that are caused when the system is attacked."

There's a big incentive to upgrade security: a California law going into effect this summer will require companies to notify—and possibly pay damages to—customers whose private information is exposed through computer breaches. Sana has a handful of competitors, including Hewlett-Packard and IBM, that are also using lessons from human physiology to automate computer security. But considering it took millions of years for immune systems to evolve, it may be a while before the market selects a winner. —*Wade Roush*

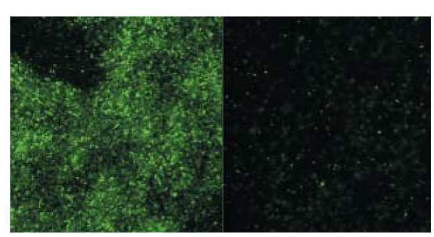
BUSTING UP BACTERIAL GANGS

BIOTECH | **By speaking the language of bacteria, researchers from the State University of New York at Buffalo have made a critical advance in the development of what could be a new class of antibiotics. Such drugs could eventually combat a host of currently incurable infections—including those caused by *Pseudomonas aeruginosa*, a bacterium that chronically infects nearly 70 percent of cystic-fibrosis patients.**

Most antibiotics block bacteria's ability to synthesize proteins or cell membranes, says biochemist Hiroaki Suga, who led the effort, but "our approach targets a completely different system." That system is a means of communication that many species of bacteria use to gang up on their hosts. Alone, these bacteria are often harmless and susceptible to regular antibiotics. But once they reach a critical density and begin to communicate through chemicals they emit, they cooperate to boost their virulence and evade traditional treatments by, for example, forming slimy biofilms.

Previous efforts to develop drugs that disrupt bacterial communication have focused on naturally occurring chemicals. Suga instead synthesized a library of molecules from scratch by tinkering with the structure of one of the communication chemicals found in *Pseudomonas*. Several of Suga's new molecules blocked the bacteria's conversation; such molecules could be used with conventional antibiotics to more effectively target the microbes.

Suga's molecules aren't strong enough to be used as drugs, says the University of Texas at Austin's Walter Fast, a medicinal chemist, but their development marks an important step forward. And, Fast says, "Hiro's approach is definitely generalizable to other bacteria." Suga has filed a patent on the technology and is fielding corporate interest. "We hope to discover more potent antagonists," he says, "so that we can get closer to developing a real drug in the future." Such drugs could bust up even the toughest bacterial gangs. —*Rebecca Zacks*



Biofilms (left) blocked (right) by new molecule.

CHEMISTRY & BIOLOGY, VOL 10, NO 1, 2003, PP81-89, SMITH ET AL: "INDUCTION AND INHIBITION OF PSEUDOMONAS AERUGINOSA..." 1 FIGURE (GANGS); JAMES YANG (ILLUSTRATION)

DB2. Information Management Software
See DB2 software connect data, near and far.
See DB2 software connect formats, old and new.
See DB2 software create insight, again and again.
Can you see it?
DB2. It's the ultimate portfolio of real-time information management software. You can now leverage every scrap of data, no matter where it is, or what it is. You see it all, as if it resided in a single place. Insightful and open, DB2 lets you use and build on what you already have, whether it's IBM, Oracle or Microsoft® — goodbye "rip and replace." For a DB2 Software Information Kit, visit ibm.com/db2/seeit
@business on demand™ software
IBM®
IBM, DB2, the e-business logo and e-business on demand are registered trademarks or trademarks of International Business Machines Corporation in the United States and/or other countries. Microsoft is a registered trademark of Microsoft Corporation in the United States, other countries, or both. Other company, product and service names may be trademarks or service marks of others. ©2003 IBM Corporation. All rights reserved.

THE END OF END-TO-END?

One of the fundamental design principles of today's Internet is so basic and so important that few users have ever heard its name; they just assume its existence. It's called "end-to-end," and some disturbing new developments are putting it in jeopardy. The end-to-end principle asserts that information pushed into one end of the Internet should come out the other without modification: the Net should act like a big, fat, dumb, digital pipe.

End-to-end operates on many levels. When you try to download a news Web page, for example, the two ends might be CNN's server and your browser. End-to-end dictates that the Internet shouldn't modify CNN's data packets as they move through the network. It thus guarantees that the page you receive is the same one CNN sent. Who could argue with that?

Many people, it turns out. End-to-end pushes a lot of power to the endpoints, but it also saddles them with some important duties. One such responsibility is security. If some hacker sends you an "attack packet," it's the job of the network to deliver that packet, no questions asked. Too bad if you haven't installed the security patch. That sounds harsh, but it is preferable for users to have this kind of control than to cede it to network administrators.

For a good example of a network that's not end-to-end, think of today's cell-phone networks. When I call my friend Jesse's cell phone, I call a phone number that's out in San Francisco. But the network knows that Jesse is actually in Boston: the call gets routed out to California then back to Boston, and Jesse's phone rings. All of this involves a tremendous amount of work on the part of the network—too much work for end-to-end. When I talk, the network takes my voice, compresses it, turns it into packets, and sends those packets down a low-bandwidth digital wireless network to Jesse's phone. The quality of what he hears is determined by the network, not by our phones.

If the cell-phone network were end-to-end, my phone would use a registration server to find where Jesse's phone is located. It would then open up a channel to his phone, negotiate with his phone to find a mutually acceptable voice compression scheme, and the two phones would start exchanging digital packets. Suddenly the network is dumb and the cell phones are smart.

So what's the advantage of end-to-end? Innovation. With an end-to-end cell-phone system, Jesse and I could upgrade to a better voice compression system just by buying new phones: nothing else in the network would have to be modified. We could also add three-way or four-way or even five-way calling, just by sending out more packets. You can't do either of these with today's cell-phone networks.

Of course, if Jesse and I have end-to-end phones, we're not limited to using cell-phone networks. We could just as easily use the Internet through wireless Net access at a university or a Starbucks. And that's the real threat of end-to-end: by putting the intelligence in the endpoints, end-to-end turns the cell-phone network—or any other network—into a commodity.

On the Internet, end-to-end promotes competition by making it easy for users to switch from one network provider to another. If I don't like the service I'm getting from my broadband digital subscriber line (DSL) connection, I can swap it out for a high-speed cable modem. Sure, my computer's Internet Protocol address will change. But thanks to end-to-end, that address really doesn't matter.

End-to-end is such a basic principle that just about any tinkering with it is bound to cause problems. Consider those Internet service providers that have toyed with blocking unsolicited junk mail: a few customers wanted their spam and resented any e-mail filtering by the provider. Other customers discovered that some legitimate e-mail was accidentally being filtered out along with the tasteless promotions for Viagra and cheap refinancing *(see "Spam Wars," p. 32)*.

The basic principle underlying the Internet promotes competition and makes it easy for users to switch from one network provider to another. That's why some companies want to kill it.

Another way to break end-to-end is to modify packets so that they go somewhere other than their originally intended destinations. That's what the government of China did earlier this year when it ordered the country's Internet service providers to replace Google's home page with a China-based search engine. Packets were intercepted and rewritten on the fly. China was thus forcing the service providers to violate the end-to-end principle: it shouldn't be the job of the network to reroute your packets to a competing Web server or block them because the content is deemed illegal.

Nevertheless, most Internet service providers would like to be able to violate end-to-end as they see fit—blocking spam, filtering out viruses, and perhaps even suppressing advertisements. They would like to make customers dependent on these "enhanced" network services so that it would be harder than ever to switch providers. Then they might start dabbling in other end-to-end infringements, like rewriting the results of Google queries, inserting advertisements directly into your e-mail, and even mining your Web-browsing habits so that they can more easily target advertisements.

Whenever you hear a company bragging about the great services it can offer directly in its network, understand that it is trying to kill end-to-end. Personally, I'd rather have a dumb network, a pair of smart endpoints, and a future.

SPAM WARS

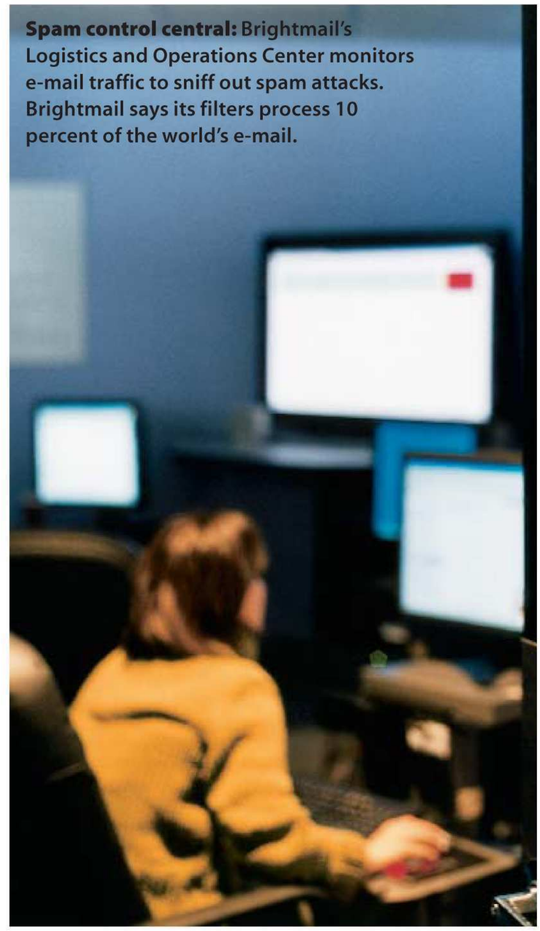
SPAM KING: Alan Ralsky spewed tens of thousands of e-mail sales pitches per hour, bringing on the wrath of Verizon.

SPAM FIGHTER: CipherTrust's Paul Judge, chair of the Anti Spam Research Group, concedes that defenses against spam can lead to more being sent.

JUNK E-MAIL NOW ACCOUNTS FOR MORE THAN HALF OF ALL MESSAGES SENT AND IMPOSES HUGE PRODUCTIVITY COSTS. NEW WEAPONS ARE HELPING STEM THE TIDE, BUT THE SPAMMERS ARE A WILY AND WILLFUL BUNCH, AND AN ONLINE ARMS RACE IS SPIRALING OUT OF CONTROL.

BY EVAN I. SCHWARTZ

Operating 20 computers in an abandoned schoolhouse in Rockford, IL, Jay Nelson worked with relatives to set up more than a dozen shell companies, renting equipment and Web hosting services using aliases such as "Art Fudge." Nelson and his associates then "hacked into AOL e-mail accounts," states one legal motion filed by AOL, and overwhelmed members with links to pornographic Web sites such as pamsplayhouse.com.


Spam control central: Brightmail's Logistics and Operations Center monitors e-mail traffic to sniff out spam attacks. Brightmail says its filters process 10 percent of the world's e-mail.

In 1999, AOL won a court injunction barring Nelson from such activities and fining him $1.9 million; nonetheless, he and his colleagues subsequently sent another billion e-mail messages—triggering 25 percent of AOL's spam-related customer complaints over the next two years.

Alan Ralsky, by contrast, seems almost respectable. While trying to overcome a past littered with fraud convictions, a court-ordered fine, personal bankruptcy, and a brief jail stint, Ralsky in 1997 heard about a new Internet opportunity. Repudiating pornography to his wife, Ralsky rented mailing lists and set up servers in his basement, according to media interviews he gave last year. Pitching mortgages, vacations, and online pharmacies and casinos on behalf of others, he boasted of thousands of dollars per week in sales commissions. After moving into a $740,000 house in a Detroit suburb, Ralsky set up another basement operation that was soon spewing tens of thousands of messages per hour, relayed through servers in Dallas and in Canada, China, Russia, and India. In 2001, Verizon Internet Services sued Ralsky, charging him with unauthorized use of its network.

Nelson and Ralsky are just two of the many faces behind spam. But according to Jon Praed, an attorney with the Internet Law Group, an Arlington, VA, firm hired by the plaintiffs in both of these cases, bigtime spammers have a common profile. "They have not been successful in anything else," he says. "They are hackers gone bad, or they are crooks gone geek." They also sit at the center of far-flung conspiracies to conceal their actions. (Neither Nelson nor Ralsky returned phone calls from *Technology Review.*)

The spam crisis is hardly a secret. But few could have imagined it would get this bad this fast. More than 13 billion unwanted e-mail messages swamp the Internet per day, worldwide. This tsunami of time-wasting junk will be a $10 billion drag on worker productivity this year in the United States alone, according to San Francisco-based Ferris Research. In a perverse analogy to Moore's Law of microchip processing power, the number of daily spam messages is doubling roughly every 18 months, according to the Radicati Group, a Palo Alto, CA, market research firm specializing in electronic messaging. Having risen from 8 percent of all e-mail in 2000 to more than 40 percent by the end of 2002, spam has now reached a majority, according to studies from several anti-spam software companies. Conceivably, spam could soon represent 90 percent of all e-mail, says David Heckerman, who heads the Machine Learning and Applied Statistics group at Microsoft Research, which is working on anti-spam technologies. If that happens, he says, "a lot of people will just stop using e-mail."

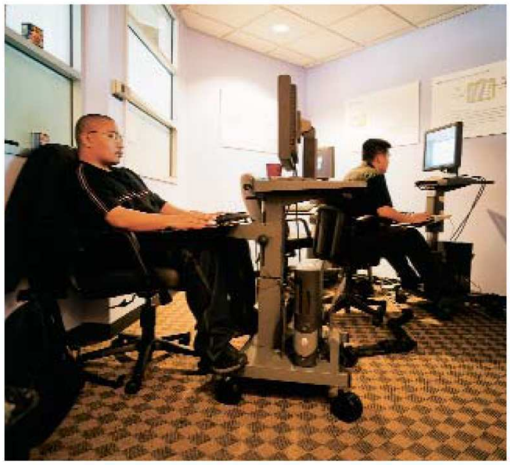
"Spammers are gaining control of the Internet," says Barry Shein, president of Brookline, MA-based The World, which started in 1989 as the first commercial provider of dial-up Internet service. Shein has been spending an increasing number of nights and weekends—the witching hours for spammers—trying to block barrages of spam that appear so suddenly that they threaten to overwhelm his service. He's constantly adding new spammers to a "blacklist" used to block all e-mail from rogue Internet addresses, but that's a Band-Aid. "They change their network identities every couple of hours," and then sometimes launch "revenge attacks," Shein says. And spammers are ever alert to fresh prey: according to a study conducted by the Federal Trade Commission, someone who uses a brand new e-mail address in an online chat room could get hit with spam as quickly as nine minutes later.

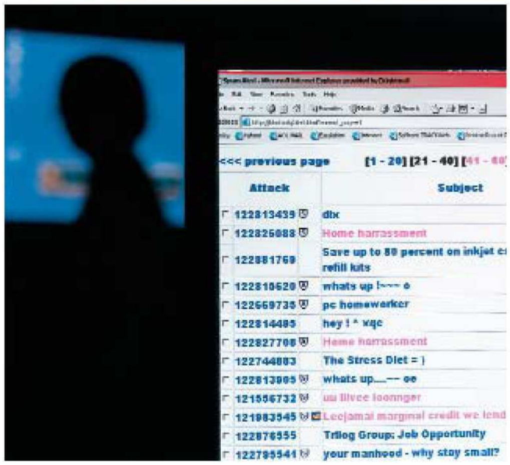
The problem could easily grow beyond anyone's control. "Our concern is not so much for the porn and the herbal Viagra as it is for the legitimate businesses," says John Mozena, cofounder of the Coalition against Unsolicited Commercial E-mail (CAUCE), an advocacy group. "There are 24 million small businesses in the U.S. If just 1 percent got your e-mail address and sent you one message per year, you'd have 657 additional messages in your in-box every day. That is our nuclear-winter scenario."

SOFTWARE WHIZZES ARE RUSHING TO FORM TEAMS AND COMPANIES TO DEVELOP BETTER WAYS TO HALT PROLIFERATION OF JUNK E-MAIL. BY 2007, SPAM-STOPPING SHOULD GROW TO A $2.4 BILLION BUSINESS.

To avert such a catastrophe, electronic warriors are fighting the scourge of spam using three principal tactics. The first involves the rapid adoption of spam-blocking-and-filtering software by consumers, corporate networks, and Internet service providers. Anti-spam software is expected to grow into a $2.4 billion industry by 2007, up from about $650 million now, according to a Radicati Group forecast. But that alone won't win the war. The second, newer approach involves instituting more drastic changes in the way e-mail and the Internet work, perhaps imposing new costs to send mes-

PREVIOUS SPREAD: AP PHOTO/PAUL SANCYA (RALSKY); SCOTT JOLLIFF (JUDGE). THIS SPREAD: TIMOTHY ARCHIBALD





sages or developing the ability to trace e-mail messages like phone calls.

The third tactic is a legal one, involving not only better law enforcement and prosecution of spammers but even a ban on all unsolicited commercial e-mail. To beat back the persistent, rising tide of spam, it's probably necessary to engage on all three fronts at once. "We move based on what we anticipate from the enemy, and then the enemy reacts," says Microsoft's Heckerman. "We're already up five levels of prediction." Everyone expects further escalation—while hoping that e-mail as we know it won't be destroyed in the process.

An Anti-Junk Arsenal

As one of the most daunting computer science problems to come along in years, the spam jam has triggered the Internet's version of a Manhattan Project. Hundreds of software whizzes are forming teams and companies in search of the ultimate way to halt mass proliferation. At the first-of-its-kind Spam Conference at MIT in January, the overcapacity crowd of almost 600 was speckled with PhDs writing scientific journal entries, young programmers wearing beards and backpacks, and P.R. pros touting the latest anti-spam services and software. The scene struck some participants as rather pathetic. "There are some very bright people here," The World's Shein told the conferees, "and what are you spending your time doing? Blocking penis enlargement ads."

Despite deep divisions among this assemblage on who has the best tools for eradicating spam, there's broad consensus on one point: if there's one thing worse than a piece of junk e-mail, it's the prospect that a spam filter will stop a legitimate message from reaching its recipient. That's why there are two important numbers one needs to know about the spam filters now in use or under development: the filtration percentage (the proportion of junk mail blocked) and the false-positive rate (the proportion of normal mail blocked). A 95 percent filtration rate is considered good, according to Paul Judge, head of the Anti Spam Research Group, started in February as a new branch of the Internet Research Task Force, a professional society. Many filters claim even higher filtration rates, he says, but those tend to run the risk of the unacceptable false-positive rates of .1 percent or higher—meaning that one in 1,000 normal messages would be lost.

Spam fighters are relentlessly adding new weapons to their arsenal. San Francisco-based Brightmail maintains one of the most widely used filters, which has been installed on corporate e-mail servers as well as the user networks of EarthLink, Verizon, Comcast, and Microsoft's Hotmail. The filter processes about 10 percent of the world's e-mail flow, says Enrique Salem, the company's CEO. Brightmail has set up more than one million randomly generated "decoy" e-mail addresses, such as Dxodt19@anydomain.com. Since no human is attached to these accounts, no one can possibly claim that their owners ever authorized a marketer to communicate with them. Within days, weeks, or sometimes months, these phony addresses will begin receiving spam.

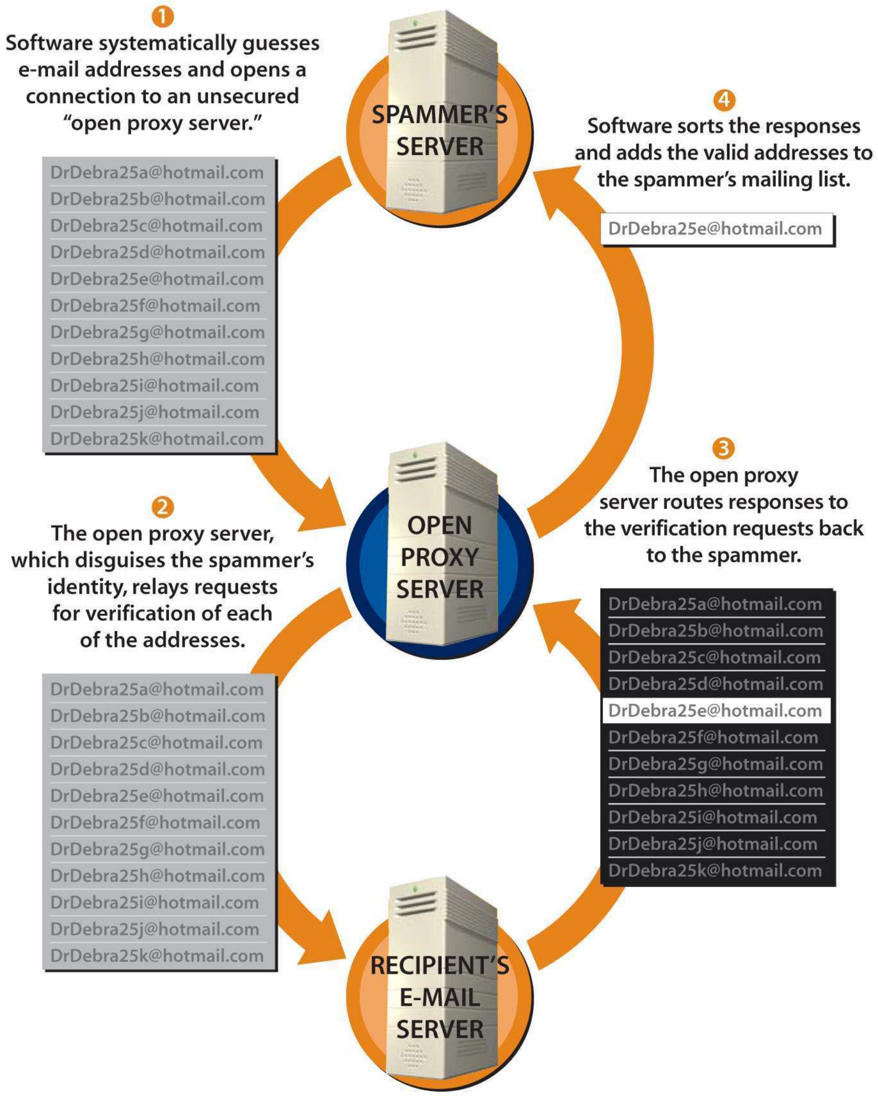
How can an e-mail address that's neither listed nor used start receiving spam? The answer is the "dictionary attack." So-called spambots not only harvest e-mail addresses posted on Web sites but connect to the major Internet service providers and systematically send standard address verification requests to guessed addresses, beginning with "aaa, aab, aac," or by trying "DrDebra25a, DrDebra25b, DrDebra25c." Such programs are often included with spam kits sold by organized syndicates. Whenever these programs fail to receive a "user unknown" type of message in reply, they add that address to a list of valid addresses, to be sold to other spammers *(see "Spreading Spam," p. 36)*.

An Internet service provider can sometimes detect such a breach and throw the attacker off the system, but the attacker will attempt to connect seconds or minutes later, from a seemingly different Internet location. According to the Spamhaus Project, a U.K.-based volunteer organization funded by a British Web hosting company, earlier this year both Hotmail and MSN were buffeted by such an attack at the rate of three to four tries per second, round the clock, for at least five months straight. (Microsoft, which runs both of the targeted services, says it has identified the alleged perpetrators and is pursuing legal action in U.S. district court in San Jose, CA.)

Brightmail's decoy method is aimed at minimizing the damage of such attacks.

Spreading Spam

A spammer harvests valid e-mail addresses using a "dictionary attack."



FRED DUPOWERS

When the in-box of Dxodt19@hotmail.com receives a message, Brightmail's software compresses that message into a unique 512-bit "signature," which is added to the database of known spam. The database is updated constantly, and a new version of it is transmitted several times per hour to Brightmail's more than 600 corporate customers. Any message that comes reasonably close to matching a known spam signature is automatically flagged as unsolicited. Eventually these pieces of presumed junk are deleted en masse. "It's like a sting operation," Salem says.

Brightmail excels in its extremely low false-positive rate. It will block only about one in a million legitimate messages, for a rate of .0001 percent. The big shortcoming of this kind of filtering is that it doesn't do a terribly good job of actually blocking junk. A new piece of spam, or even a significant twist on an old spam, will probably make it through. Indeed, Brightmail's Salem claims only a 92 percent filtration rate—and large customers such as Microsoft and EarthLink peg the actual rate at more like 70 percent. That's why Brightmail is only used as a rough filter—and why it doesn't come close to tackling the overall problem.

Smarter Shields

Seeking a more perfect form of relief, tens of thousands of users have downloaded open-source filters (most popularly, Spam Assassin) or purchased commercialized versions such as McAfee's SpamKiller. A collection of statistically valid rules created by humans, these "heuristic" filters stand guard at the user's in-box and scan every incoming message for tip-off terms such as "Viagra," "V1AGRA," or even "V*I*A*G*R*A," plus improbable return addresses, strange symbols, embedded graphics, and fraudulent routing information, indicating the message is of dubious origins. After applying hundreds of rules, the filter scores each message, discarding those whose scores exceed a threshold value. Spam Assassin and SpamKiller typically exhibit filtration rates higher than 95 percent and false-positive rates of about .1 percent, according to Matt Sergeant of MessageLabs, a maker of Spam Assassin improvements.

This relatively high false-positive rate, however, is troubling to some users. After all, much legitimate e-mail has some of the same traits as spam. Sergeant concedes that newsletters that were requested by users will occasionally be discarded. That flaw has led to novel solutions such as collaborative filters, in which users vote as to which messages should be deemed spam.

SpamNet, from San Francisco-based Cloudmark, is one example of a program that deploys democracy in this way. An add-on to Microsoft's Outlook e-mail program, SpamNet starts filtering spam automatically upon installation. If enough trusted users designate a message as spam, that message ends up in the spam folders of Cloudmark's entire base of 420,000 users. "When a new person joins, they get the benefit of the community," says Vipul Ved Prakash, Cloudmark's founder and chief scientist. False positives are rarer under this approach, and users also have the option of clicking "unblock" on any messages in their spam folders. But there are drawbacks: SpamNet demands a higher level of user vigilance, and it requires that Cloudmark's remote servers examine all incoming e-mail before passing it on.

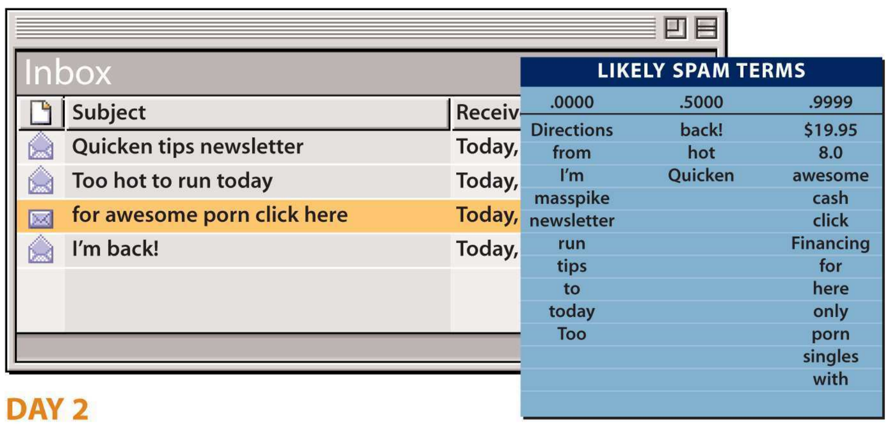
To fend off spam that penetrates other defenses, computer scientists have turned to the 18th-century probability theory of English mathematician Thomas Bayes. Published in 1763, two years after his death, Bayes's "Essay towards Solving a Problem in the Doctrine of Chances" provides a blueprint for determining the likelihood of future events. Since one person's spam can be another person's invitation to a pleasurable afternoon, Bayesian spam filters learn over time what each individual considers unwanted e-mail.

Stopping Spam

Trainable "Bayesian" filters are emerging as one of the most potent anti-spam weapons.

DAY 1

The filter notes which messages you open and assigns terms from subject lines probabilities of indicating spam. In this first batch, "Directions from masspike" is assigned the lowest probability of indicating spam; the unopened messages are assumed to be spam, and the words in their subject lines are classified accordingly.



DAY 2

The user's treatment of the next day's batch of e-mail helps the filter refine its probabilities. Words that have non-spam uses (like "hot") are no longer sure signs of spam. Using such a Bayesian filter for a few days yields high filtering rates with few false positives.

When a user deletes several unopened messages about mortgage refinancing, for instance, a Bayesian filter learns to discard e-mail with that kind of terminology. If you typically do read such messages, however, the filter will take note of that and consider it normal e-mail.

Because Bayesian filters can be trained, their effectiveness improves over time, typically attaining filtration rates of 99.8 percent, along with a false-positive rate of a mere .05 percent. "If everyone's filter has different probabilities of different messages getting through, it makes it harder for the spammers," says Paul Graham, an independent Cambridge, MA, programmer. Last August, a link to Graham's article "A Plan for Spam" on slashdot.org jump-started a rush to Bayesian filtering. These kinds of filters, Graham says, will break the business model of the spammer. It costs about $200, he continues, to send one million messages—an endeavor that typically yields about 100 responses. If those 100 people spend an average of $2 each, the spammer breaks even. The goal, Graham says, is to drive response rates down to around one in a million so that "it would no longer be economical for a spammer to consider such a business proposition."

Microsoft Research has taken this probabilistic approach even further. Standard, so-called naïve Bayesian filters treat each word or feature in an e-mail independently, but Microsoft claims its new filter, which is offered as an option in MSN 8 software, learns probabilities for words, phrases, and other distinguishing characteristics that commonly appear together. It might flag messages containing the phrase "make money from home" and "click here" that are sent from servers based in Hong Kong and that have random characters in the subject line. Microsoft's Heckerman claims that, by correlating patterns, his filter exhibits an even lower rate of false positives.

The monkey wrench is that spam is not an inanimate adversary, but rather a tool of wily and willful humans. In fact, the very effectiveness of spam filters may actually be making the problem worse. If half of a batch of spam gets thrown into the digital garbage can, the spammer will tend to respond by sending twice as much spam the next time. "As you put more filters in place, spammers become more determined, and the spam will increase," says the Anti Spam Research Group's Judge, who is the chief technology officer at CipherTrust, an Alpharetta, GA-based provider of e-mail security systems.

To balance the higher volume, Judge says, spammers simply find ways to lower their costs, such as enlisting servers based in China or India, where labor is cheap. What's more, as spammers mount a counterattack against Bayesian methods, spam is tending to look more and more like non-spam. For example, a message that says, "Hi Jim, have you seen the party pictures—take a look!" may not raise red flags, because it doesn't contain any obvious spam terms. When spam begins to look exactly like messages from friends and colleagues, filters may fail.

Crippling the Attackers

That's why anti-spam researchers are cooking up more-systematic treatments. Referring to spam as a "plague," Mark Petrovic, vice president of R&D at Internet service provider EarthLink, notes that today's e-mail system was designed 20 years ago for small numbers of people who already knew one another. "The possibility of sending body part enlargement ads was unheard of," he says. Stemming the tide of spam, he says, will "require a cooperative solution to augment the basic way e-mail works."

The most widespread of these measures is a blacklist of the sort used by Shein and other Internet service providers. Also maintained by startups such as SpamCop and NetBlocks, and by nonprofits such as CAUCE and Spamhaus,

blacklists are collections of Internet Protocol addresses, domain names, and server farms that have been implicated in spewing spam; any mail originating from these tainted places will be blocked. But blacklists are imprecise: they often fail to keep pace with spammers, who constantly falsify their network locations, while sometimes blocking legitimate users. Indeed, blacklists sometimes halt e-mail from entire countries with high spam rates. E-mail originating in China and South Korea, in particular, has periodically been blocked from much of the Internet.

The inverse of the blacklist is the white list—a preauthorized address book maintained by users. An option in AOL 8.0, for instance, causes any message from senders not on the high-priority list to be discarded. This method also tends to trash e-mail you might want, though, and requires a high degree of maintenance; every time you make a new contact, you have to add a name to the white list. Aside from these drawbacks for their users, blacklists and white lists also are "wreaking havoc" on legitimate mass e-mailers, says Paul Soltoff, CEO of SendTec, a direct-marketing firm. After all, many companies (*Technology Review* among them) send out electronic newsletters and other promotional materials. These aren't as obnoxious as the come-ons that most of us consider spam, and yet they are just as vulnerable to being blocked through the widespread use of blacklists and white lists.

Another drastic anti-spam measure strikes at the heart of the Internet's culture: imposing new costs on sending e-mail. "Paying to send e-mail may be anathema to almost everybody," says Robert Hettinga of Internet Bearer Underwriting, a startup in Boston. "But eventually, bits of money will be attached to e-mail messages." Just as paper mail requires postage, e-mail would require e-stamps. A charge of one-tenth of a cent per e-mail, for instance, would hardly be noticeable to ordinary users but would levy a $1,000 tax on someone sending a million messages at once. Any piece of e-mail sent without an e-stamp would be automatically blocked.

Others favor imposing a cost not in dollars but in the sender's computer time. Your PC would have to solve a quick mathematical problem for each message it transmits, barely affecting senders of normal quantities of e-mail but crippling a spammer's microprocessor. Such a "computational cost" approach is being developed at Microsoft Research and in an open-source effort called Camram *(see "Making Spam Expensive,"* TR *April 2003).*

The World's Shein proposes an Internet market trade association, which would be an "e-mail clearinghouse," run by a group of e-mail providers. Such an organization would sell legitimate bulk mailers special license codes in return for royalties based on the size of the mailings they are sending. Spammers who buck the system would be tracked down and sued by clearinghouse lawyers using funds set aside from the royalty pool. "The goal is to monetize the processing of bulk e-mail," Shein says. He derives the idea from the long-established model by which radio stations and performers pay royalties to songwriters based on the formulas of another clearinghouse: the American Society of Composers, Authors, and Publishers. Elements of such a plan are already being adopted by the big three of e-mail providers—Microsoft, Yahoo!, and AOL—who announced in April that they are banding together to develop a way of creating a white list for legitimate marketers. The group has yet to announce whether participating marketers will pay to maintain a new infrastructure, but Shein guesses that things are heading that way.

For such a plan to work, future e-mail will have to be traceable. The telephone system has survived, in part, because there have always been ways to track phone calls back to their sources and find those who abuse the network. "Filtering e-mail without being able to establish identity is essentially futile," says EarthLink's Petrovic. He cites the problem of spam masquerading as real e-mail. "If my wife says, 'I'd like to spend some time with you this evening,' I will react differently than if a stranger says the same thing. I need to know who is talking to me before I can evaluate the meaning of the message." Indeed, Petrovic adds, the anonymity of e-mail is central to the spam phenomenon. If we cannot determine who is sending messages, all other spam-blocking measures will ultimately fail.

Establishing such traceability would require fundamental changes to the basic protocol that governs all e-mail transmission. Called the Simple Mail Transport Protocol, or SMTP, it is the 20-year-old language that virtually all e-mail software speaks in order to move messages around

Seven Ways of Sifting Spam

FILTERING APPROACH	COMPANY	PRODUCT
"Signature-based" filtering	**Brightmail** (San Francisco, CA)	Anti-Spam
	Cloudmark (San Francisco, CA)	Authority
	SurfControl (Congleton, England)	E-mail Filter
"Collaborative" filtering in which users vote on which messages constitute spam	**Cloudmark** (San Francisco, CA)	SpamNet
"Gateway" corporate network that intercepts spam before it reaches desktops	**Computer Associates** (Islandia, NY)	eTrust
	CipherTrust (Alpharetta, GA)	IronMail
	ActiveState (Vancouver, British Columbia)	PureMessage
	NetIQ (San Jose, CA)	MailMarshal
	IntelliReach (Dedham, MA)	Message Screen
"Heuristic," or rule-based, content filtering in which a filter scans e-mail for junk mail tip-off terms	**McAfee Security** (Santa Clara, CA)	SpamKiller
	SpamAssassin	open-source software
	Elron Software (Burlington, MA)	Message Inspector
	Matterform (Española, NM)	SpamFire
Bayesian, or probability-based, filtering that learns each user's definition of spam	**Microsoft** (Redmond, WA)	MSN 8
	Spammunition	freeware
"Circle of trust" clearance, which only lets through e-mail from preauthorized users	**Habeas** (Palo Alto, CA)	Sender Warranted E-mail
	AOL (Dulles, VA)	white-list feature
"Vaccinating," which hides users' e-mail addresses from spammers	**Matterform** (Española, NM)	Spam Vaccine
	Sneakemail (Marblehead, MA)	Sneakemail

Coping with masses of junk e-mail poses a daunting technical challenge for computer scientists, who exchanged war stories at MIT in January at the first ever Spam Conference.

COURTESY OF GERALD OSKOBOINY

the Internet. If all network providers switch to an "authenticated SMTP," as EarthLink's Petrovic calls it, only an e-mail with a verified return address and from a valid domain name would be able to get to its desired recipient.

The Legal Front

Technology alone will never win the war. Ninety percent of spam is sent by fewer than 200 people, according to Mozena of CAUCE, the anti-spam coalition. That represents an astounding degree of concentration, but virtually everyone who fights spam for a living agrees it is roughly correct. The implication is clear: spam is a crime-fighting problem akin to the prosecution of the small number of malicious hackers who crack into networks. "These are human beings generating these messages," Mozena says. "It's not as if the Internet is broken. You can't address social problems solely with technical means." He believes that the spam plague is a criminal-justice dilemma that can be eradicated only with the active participation of legislatures and courts.

New laws, though, have yet to make much of a dent. Last year, the European Parliament passed a directive suggesting that member countries require marketers to ask permission from users before sending pitches through e-mail. So far, Austria, Denmark, Finland, Germany, Greece, Italy, and Norway have enacted such "opt-in" anti-spam legislation. But since so much spam is sent from the United States through Asia-based servers, these laws have had little effect. In 2000, the U.S. House of Representatives voted 427 to 1 to pass an anti-spam bill. But instead of including a strict opt-in provision, the bill required consumers to request the removal of their addresses from each marketer's e-mail list. After privacy advocates denounced this "opt-out" bill as useless, it died without reaching the Senate. At least two spam bills are now alive in Congress, but there is still no consensus among lawmakers on whether the government can effectively outlaw spam—or even that it should.

In April, the Federal Trade Commission held a conference to help decide how best to approach this crisis. Brian Huseman, an FTC staff attorney, says the commission has prosecuted spammers who have sold bogus wares, failed to live up to their claims, impersonated legitimate organizations, or engaged in other deceptive practices. But since the agency is mainly charged with prosecuting fraud cases, it is powerless against spam that sells legitimate products. "There is no federal law that prohibits unsolicited commercial e-mail," Huseman says.

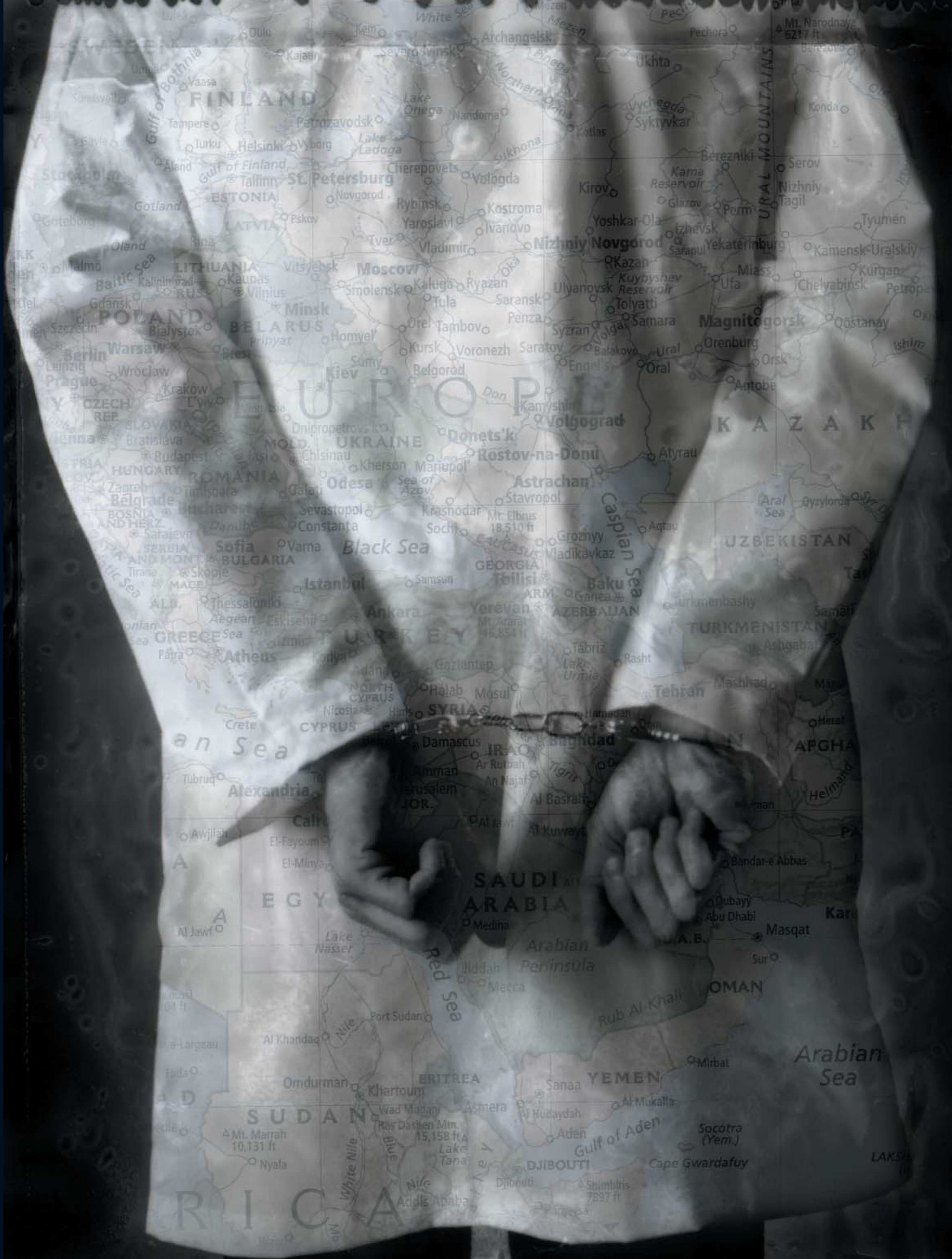
Until such a law is passed, lawyers will continue to rely on precedents from similar cases, says Jon Praed of the Internet Law Group. He believes that indiscriminate mass e-mailing is "already illegal in all 50 states" based on centuries-old Common Law that prohibits unauthorized use of someone else's property—in this case, computer networks.

Armed with this argument, AOL pursued porn spammer Jay Nelson, both before and after he and his cohorts violated the 1999 court order. Since spam cases can be prosecuted anywhere damage occurs, AOL chose its hometown district court in Alexandria, VA. In October 2002, the judge held the coconspirators in contempt and awarded AOL $6.9 million in damages and fees on top of the original $1.9 million finding, according to court documents. That figure was topped in May when EarthLink won a $16.4 million judgment against Howard Carmack, a Buffalo, NY, spammer; a week later, he was arrested on charges of identity theft. Praed says spammers cannot skirt the payments by filing bankruptcy, and that the plaintiff can "hound" the guilty parties until the money is collected, preventing them from buying houses and cars. "We need to make the spammers realize they made a mistake and to discourage others from doing it," he says.

Detroit-based spammer Alan Ralsky, however, remains active. Instead of spending more time and money bringing Ralsky to court, Verizon last October decided to settle its case against the man that some call "the spam king." In return for Ralsky's paying an undisclosed sum and promising to avoid Verizon's network, the lawsuit was dropped—leaving Ralsky firmly in business.

Furious anti-spam activists posted Ralsky's home and e-mail addresses online, and soon he was deluged with piles of printed catalogues and junk mail. Yet he appears undeterred and continues to add to his list of 250 million e-mail addresses. According to his own statements, he is finding new ways to obscure his identity, laundering his Internet location data through servers in Romania and obscure parts of China. Spamhaus and CAUCE consider the 57-year-old Ralsky one of the top five spammers worldwide. "I'll never quit," he told the *Detroit Free Press.* "I like what I do. This is the greatest business in the world."

The war on spam won't be won until guys like him are somehow forced to change their minds. TR


FINLAND
Archangelsk
Ukhta
Petrozavodsk
Helsinki
St. Petersburg
ESTONIA
Cherepovets
Vologda
Kirov
URAL MOUNTAINS
LATVIA
LITHUANIA
Moscow
Nizhniy Novgorod
Kazan
Yekaterinburg
Minsk
BELARUS
POLAND
Warsaw
Berlin
Prague
Kiev
Samara
Magnitogorsk
Orenburg
Voronezh
EUROPE
UKRAINE
Volgograd
Rostov-na-Donu
KAZAKH
Astrachan
ROMANIA
HUNGARY
Odesa
Black Sea
Caspian Sea
UZBEKISTAN
Sofia
BULGARIA
GEORGIA
Tbilisi
Baku
Istanbul
Ankara
TURKEY
Yerevan
AZERBAIJAN
TURKMENISTAN
GREECE
Athens
Tehran
CYPRUS
SYRIA
Damascus
IRAQ
Baghdad
Alexandria
SAUDI ARABIA
Medina
Mecca
Arabian Peninsula
Red Sea
Masqat
OMAN
Rub Al-Khali
Arabian Sea
YEMEN
Khartoum
SUDAN
Gulf of Aden
DJIBOUTI
AFRICA

BIOTECH'S BIG CHILL

BIOMEDICAL RESEARCH IN THE UNITED STATES IS FACING A SECURITY CLAMPDOWN UNLIKE ANYTHING SEEN IN SCIENCE SINCE THE DAWN OF THE NUCLEAR AGE. PHYSICS SURVIVED COLD-WAR RESTRICTIONS, BUT THE EFFECTS OF CURRENT LIMITATIONS ON BIOTECHNOLOGY COULD BE FAR MORE CHILLING FOR U.S. COMPETITIVENESS.

In late October 2001, Tomas Foral, a 26-year-old master's student working in a pathology laboratory at the University of Connecticut in Storrs, was asked by a professor to help clean out a failed basement freezer. Foral discovered that the freezer contained several vials of cow tissue infected with anthrax. What happened next is in dispute: university officials would later say the professor told Foral to destroy the vials, while Foral maintains that the professor's instructions were unclear. In any event, he saved two of the vials for future research by putting them in another laboratory freezer.

A month later, according to media accounts, an anonymous tip led police to Foral and the saved vials. The pathology laboratory building was shut down for more than a week, the FBI began an investigation of Foral, and in July 2002 the government charged him with having violated the antiterrorist USA Patriot Act. Initiated in the wake of the attacks on the World Trade Center and the Pentagon and passed on October 26, 2001, the act contained a section that responded to the anthrax mailings and deaths that had begun early that month. The section prohibited possession of any of more than three dozen lethal biological agents—including anthrax—or genetically modified versions of them, unless it was "reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose." The penalties threatened alleged violators like Tomas Foral with a hefty fine and up to 10 years in prison.

BY DANIEL J. KEVLES

ILLUSTRATION BY STEPHEN SHEFFIELD

That section of the USA Patriot Act was just one in a sweeping set of post–September 11 provisions designed to control access to almost every aspect of science and technology—not just biology—that could conceivably aid terrorists. In another section, the act tightened regulations on foreign students and provided, among broad controls on all foreigners entering the country, $37 million for a federal electronic database—the Student Exchange Visitor Information System, first authorized in 1996 but then neglected—containing information on foreign students and visitors at U.S. colleges and universities.

A subsequent measure, passed in May 2002, increased the responsibility of educational institutions for recording information about their international students, including whether they were maintaining full academic loads, had changed programs, or had ended their studies. (Rutgers University administrator Marcy P. Cohen lamented to a reporter that she used to spend her time helping foreign students, but that now "I've become a data monitor for the government.") That June, legislation was enacted to protect the public against bioterrorism by denying "restricted persons"—including drug users, dishonorably discharged military personnel, and people suspected of involvement with terrorist organizations—access to dangerous biological agents and toxins. The law also prohibited citizens of countries designated as sponsors of terrorism (currently Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria) from accessing certain biological agents.

A deluge of regulations followed the legislation, including draft requirements issued in December 2002 that filled 50 pages of the *Federal Register* and affected universities, private corporations, and government laboratories handling any of nearly 50 "select" biological agents—for example, Ebola virus, botulism-causing bacteria, and the toxin Ricin. All the laboratories had to agree to unannounced inspections, register their agents with the government, and submit plans for training lab workers and maintaining the security of the agents. Everyone handling the agents would have to undergo a background check and obtain security clearance. The labs would also have to obtain federal approval before conducting genetic engineering experiments that might increase the resistance of an agent or toxin to drugs.

More alarming to biomedical scientists were increasing signs—beginning with an order from the White House chief of staff in March 2002 telling federal officials to keep the lid on unclassified but "sensitive" information related to weapons of mass destruction—that the Bush administration might restrict the as yet untrammeled publication of unclassified research. How aggressively that ominous initiative would be pursued remained to be seen, but the fate of Tomas Foral, a member of the Reserve Officer Training Corps, suggested that the government meant business. Although Foral said he had frozen the anthrax spores for further research, a purpose seemingly allowed by the USA Patriot Act, he escaped prosecution only by agreeing to community service and six months of probation. A letter from the U.S. attorney describing his alleged illegal act would go to his ROTC commanding officer. Foral feared that his professional future might be compromised.

Security restrictions are old hat to physical scientists, who have been dealing with similar constraints since the dawn of the nuclear age, but they are new to biomedical researchers, who have previously had to cope only with regulations affecting public health and safety. Despite security constraints, U.S. physics prospered during the Cold War, and biology may flourish similarly in the future—especially since it is receiving handsome funding ($1.5 billion to the National Institutes of Health in fiscal 2003) for research into bioterrorism.

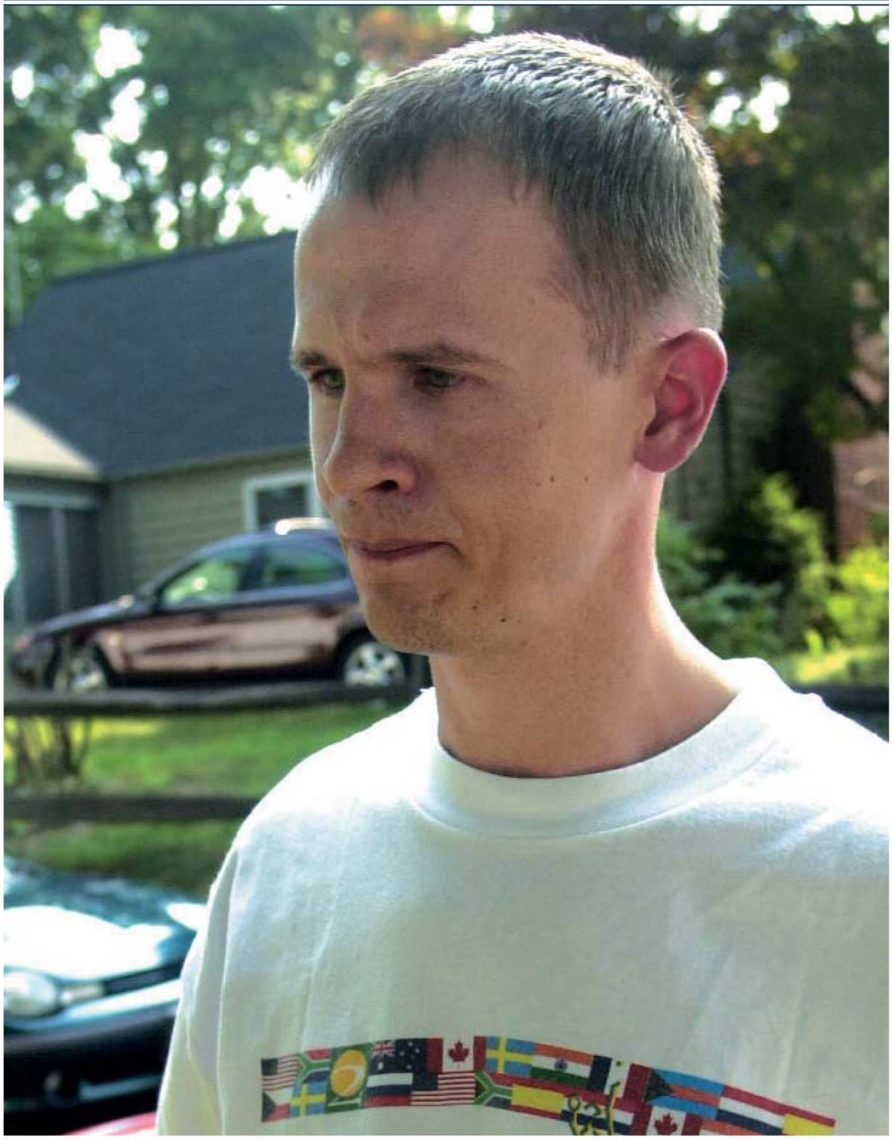
But the new restrictions, and those on the horizon, may pose difficulties for contemporary biology that are far more chilling than those that beset early Cold War physics. The current constraints on foreign students and visitors in the name of national security have already worked "serious unintended consequences for American science, engineering, and medicine," according to the presidents of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine, in a December 2002 statement protesting the government's policies. Censorship of sensitive unclassified research threatens worse effects, by menacing open communication in numerous biomedical areas—including the study of disease and the immune system. It could thus, some experts charge, threaten researchers' abilities to engineer therapies and cures—and that could place the very competitiveness of the nation's biotechnology industry in peril.

EXPERTS CHARGE THAT RESTRICTIONS ON SCIENCE AND SCIENTISTS, SOME ALREADY IN EFFECT AND SOME ON THE WAY, THREATEN RESEARCHERS' ABILITIES TO ENGINEER THERAPIES AND CURES. THAT COULD PLACE THE VERY COMPETITIVENESS OF THE U.S. BIOTECH INDUSTRY IN PERIL.

Physicists became enmeshed with national security when they built the atomic bomb in World War II and then committed themselves to maintaining nuclear superiority during the Cold War. The key object of control was information: how to obtain fissionable fuel for atomic bombs, and the workings of the bombs themselves. No one disputed that research on nuclear weapons or access to such research had to be restricted to scientists who would not risk national security by releasing classified information, either inadvertently or through espionage.

That logic was sensible on its face, but how to make it operational was highly disputed in the tense, early years of the Cold War. Communism was understood to be an international conspiracy, demanding loyalty to the Soviet Union from its adherents everywhere. The revelations of the espionage committed by the nuclear physicists Alan Nunn May and Klaus Fuchs indicated that the conspiracy reached into the heart of the nuclear-weapons enterprise in Canada and the United States. In 1947, to defend against Communist infiltration of the government, the Truman administration began requiring loyalty checks for all federal employees. The policy affected almost 60,000 U.S. scientists and engineers.

In that politically fraught climate, which yielded Senator Joseph McCarthy's reign of ideological terror, the line between liberalism and Communism was blurred, often making liberals suspect as



The accused: University of Connecticut grad student Tomas Foral froze vials of anthrax-infected cow tissue, a move that got him charged with violating the USA Patriot Act.

AP PHOTO/BOB CHILD

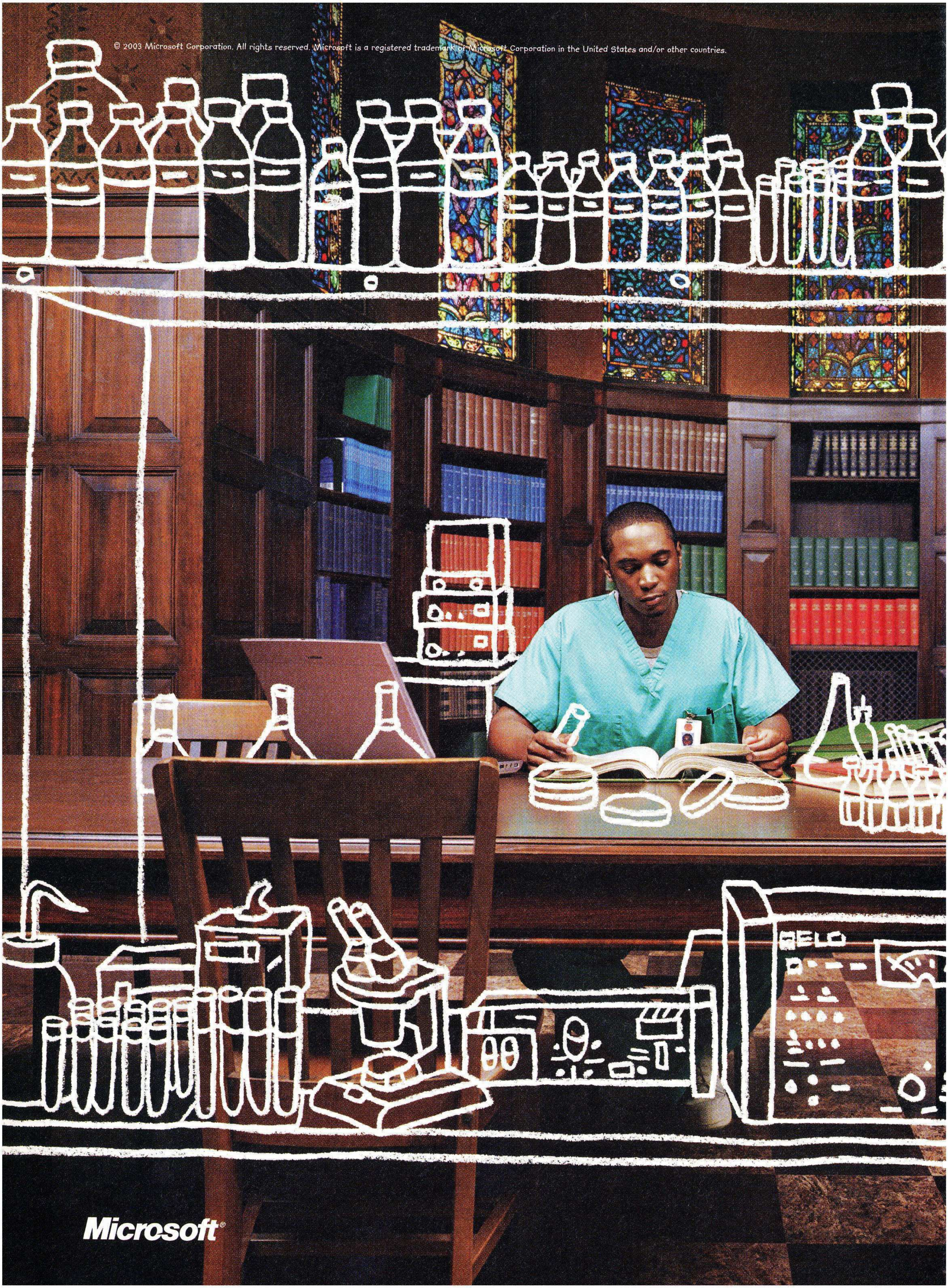
security risks and opening their activities to scrutiny by FBI investigators. Lengthy security-clearance investigations could cost scientists months of anguish and unemployment. For some, past or present political associations led to the denial of clearances or to confinement to unclassified research. For others, they produced public castigation, like the House Un-American Activities Committee's unwarranted denunciation of the physicist Edward U. Condon, the head of the National Bureau of Standards, as "one of the weakest links in our atomic security."

Worries about security led the government even to cloud the distinction between practitioners of classified and unclassified research. In 1950, some conservative congressmen tried to require security clearances for all researchers receiving fellowships from the proposed National Science Foundation. They failed, but that same year the Joint Committee on Atomic Energy successfully imposed the requirement on all applicants for Atomic Energy Commission fellowships, whether they would be engaged in classified research or not. There is always the chance, declared the conservative Republican senator William Knowland, that some student, even if engaged in nonsecret studies, might "hit upon a superduper atom bomb and be off to Russia." The State Department, determined to protect U.S. atomic secrets against suspicious foreigners, denied the Nobel laureate Paul Dirac, a member of the British atomic-energy effort but in the 1930s a frequent visitor to the Soviet Union, a visa to attend scientific congresses in the United States. It also refused the homegrown chemist Linus Pauling, an outspoken liberal, a visa for travel abroad.

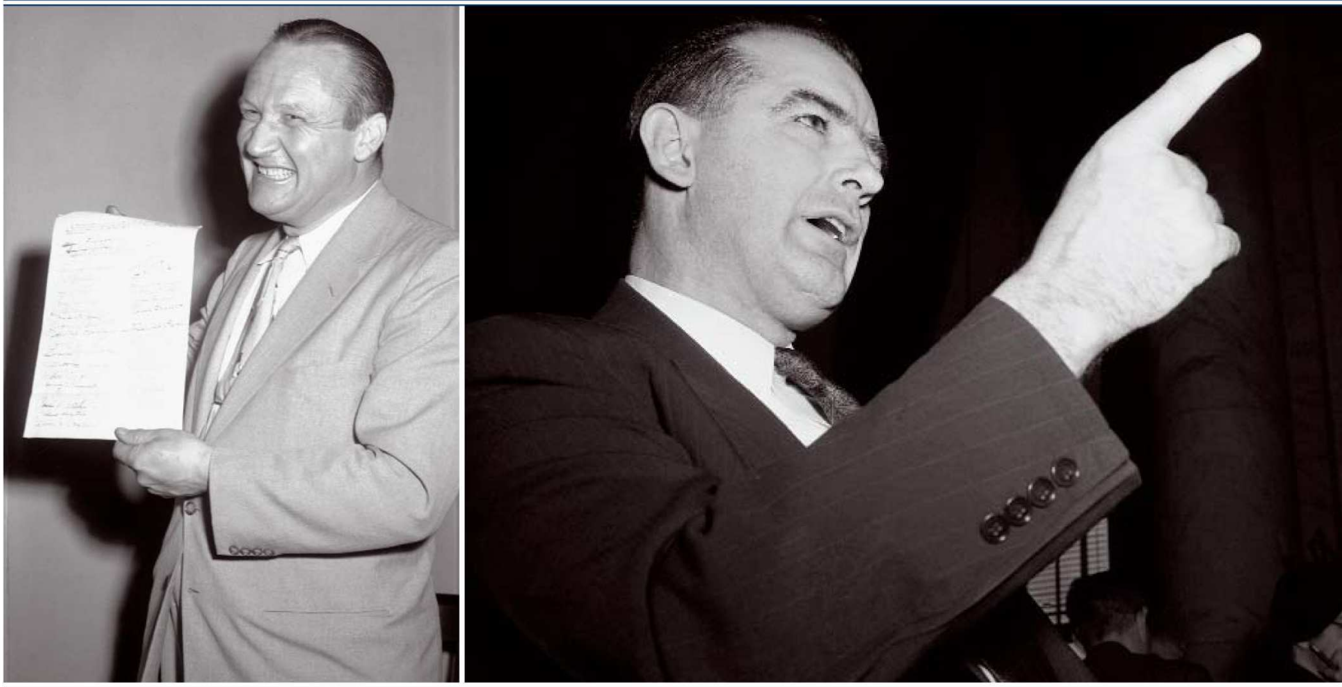
Some scientists protested the assaults on civil liberties. "The opportunity of the young scientist to develop his ideas should not be purchased at the expense of his human dignity," Albert Einstein said. But the security issue left President A. N. Richards of the National Academy of Sciences cowed. Explaining the academy's refusal to come vigorously to Condon's defense, Richards said that "the most unfortunate outcome would be to jeopardize our relations with government." And as the Cold War intensified, many scientists came to consider Communism a sufficient threat to U.S. security to warrant the curtailment of civil liberties.

Harvard University president James B. Conant, a key figure in atomic policymaking and a liberal on most domestic matters, was typical. Conant waffled on the Condon case, and in December 1948, several months after the Communist takeover of Czechoslovakia, he said, "It must be recognized that quite apart from the possibility that some individuals might be connected with this [Communist] conspiracy, others who are quite innocent of any such ties are nevertheless temperamentally naive and indiscreet and cannot be trusted with confidential information in spite of their excellent intent and high ability. The government, in resolving doubts on these matters about employees, including scientists, must settle the case in favor of the government rather than the individual. If a shadow of doubt exists, the individual should be prevented from having access to confidential information."

LIKE PHYSICISTS DURING AND AFTER World War II, many biomedical scientists today are eager to help strengthen national security. In June 2002, a committee of the National Research Council published *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, which laid out a variety of research agendas, including one in the area of human and agricultural health. Microbiologists have often been casual in managing lethal agents, keeping anthrax, for example, in glass tubes on bench tops in unlocked labs. Most biologists today seem to consider reasonable the requirement that


© 2003 Microsoft Corporation. All rights reserved. Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries.
Microsoft


we see
a promising new heart drug.
The next breakthrough in any field will result from a combination of inspiration, cooperation, luck, and especially hard work. This is why we create software that helps you find and nurture ideas, no matter how small. Because really big ideas don't always start out really big. microsoft.com/potential
Your potential. Our passion.



Fear and loathing: Cold-War-era senators William Knowland (left) and Joseph McCarthy (right) investigated scientists for Communist allegiances.

BETTMANN/CORBIS

anthrax samples be inventoried and locked up.

But many microbiologists worry that the new security regulations may be counterproductive not only to basic research and biotechnology but even to the defense against bioterrorism. Ronald Atlas, president of the American Society for Microbiology, has noted that "some researchers are now afraid to be anywhere near an anthrax culture," and that many academics are destroying their restricted agents to be sure of avoiding prosecution. Gary Bass, executive director of the nonprofit OMB Watch, which advocates greater access to government information, has observed, "We have a basic principle of right to know in this country. It is shifting, ever so subtly, to becoming one based on a need to know." Robert Iuliano, acting vice president and general counsel at Harvard, told me recently that many faculty members worry how the restrictions on foreigners may affect the openness of the campus—for example, the accustomed freedom of undergraduates, no matter their national origins, to visit any laboratory. An essential and troubling question facing American scientific leaders is how to help defend the country without damaging the vitality of basic research, biotechnology, and, indeed, higher education.

The National Academy of Sciences has been far more publicly active in dealing with the question now than in the post–World War II decade. The American Society for Microbiology has also weighed in powerfully on security issues. It has commanded attention by reason of its size—42,000 members—and of the tireless outspokenness of Atlas, an environmental biologist with experience at the intersection of science and policy. After September 11, Atlas was inundated with inquiries from scientists, government officials, and the media. "At the height of the anthrax attacks," he told me in a recent e-mail, "I was handling 70 press calls a day. I had to have two secretaries working full time to screen calls." Academic scientists were not consulted when security restrictions were inserted into the USA Patriot Act; Atlas felt they ought to have been.

Still, U.S. scientists are not toiling in the same atmosphere of suspicion that they endured during the Cold War. None is accused of being a risk to national security, the way some physicists were in the heyday of McCarthyism; none needs fear being branded a subversive simply for speaking out in defense of open and accessible biomedical science. And so they have been able to publicly take issue with the new restrictions.

But in several ways today's biologists face more difficult obstacles than physicists did in the early Cold War. Then, a scientist was made suspect by his or her political affiliations. In principle, suspicion could be allayed by repudiations of past political behavior and renunciation of current allegedly dubious activity. In contrast, what makes a scientist suspect today is his or her nationality, which is difficult to modify, or ethnicity, which is unchangeable. There is no appeal against the denial of access to selected biological agents on the basis of nationality; it applies absolutely without exception.

Foreign students are now subjected to close scrutiny in applications for visas. The State Department reportedly asks all male applicants between the ages of 16 and 45 whether they have any experience with biological weapons or have participated in armed conflicts. (Of course, a would-be terrorist would just lie, but discovery of the lie would provide grounds for prosecution and expulsion from the country.) Requests for visas, especially by male students from Arab and Muslim countries, and by anyone bound for scientific activities, often meet with lengthy delays. A number of foreign students home on vacation after having been previously admitted to the United States have found themselves stuck awaiting reentry; one doctoral candidate at Yale University who went home for the holidays in December 2002 had to wait so long for a visa that he missed the spring semester.

Visa delays and denials have already interfered with or caused the cancellation of important international conferences, disrupted careers, and slowed research

Denounced: U.S. physicist Edward U. Condon (left) and U.K. Nobel laureate Paul Dirac (right) were among many who came under suspicion.

HULTON-DEUTSCH COLLECTION/CORBIS (CONDON); BETTMANN/CORBIS (DIRAC)

projects—including, according to media reports, an anti-HIV drug, a vaccine against the West Nile virus, and sensors to detect biowarfare agents. In the long term, they could jeopardize the nation's research and training programs, which depend heavily on foreign students, and ultimately its economic competitiveness. According to 1997 figures, the latest available, foreign-born students represent a quarter of all U.S. PhDs in biology. The U.S. biotechnology industry draws abundantly on these trainees: between 8 and 10 percent of its employees are visa-holding foreigners, four out of five of whom trained at American universities.

Even if they negotiate the visa gauntlet, foreign students may find themselves investigated by the FBI if they are working in potentially dangerous biomedical research. Critics worry that under the broad terms of the USA Patriot Act, the government might claim authority to pry into student records and e-mail accounts. Visa-holding Muslim students have been complaining of harassment on their return to the United States from vacations. Students from countries believed to sponsor terrorism are fingerprinted, photographed, and required to check in periodically with the government. In an interview with the *Chronicle of Higher Education*, Omar Afzal, who advises Muslim students at Cornell University, said, "They are terrified. They come from a culture where if a policeman shows up at the door, you are being targeted to be sent to prison for a long time."

Beyond visa considerations, biomedical scientists have found especially disturbing the prospect of restrictions on the practice and publication of so-called sensitive research. In nuclear research, a line could be drawn between research that was and was not integral to national security. If the investigation of fissionable nuclei was crucial to national defense, research into the nuclei in most of the periodic table was not. It remained open and unclassified.

In contrast, the line in biomedical research is blurred, because results in almost any area of basic molecular biology may be fuel for bioterrorism. The problem has been illustrated by several recent publications. Early in 2001, in an article in the *Journal of Virology*, Australian scientists reported that the insertion of a gene into the mousepox virus had unexpectedly made the virus lethal to mice previously resistant to it. Intended to make mice infertile, the experiment suggested how to engineer human viruses to bypass the immune system. In a paper in the *Proceedings of the National Academy of Sciences*, in June 2002, Ariella Rosengard of the University of Pennsylvania described the synthesis of a protein in the smallpox virus that presumably enables it to evade the immune system. The next month, *Science* published a report by a microbiologist at the State University of New York at Stony Brook, detailing how to assemble a poliovirus from scratch using commercially available chemicals and DNA synthesis machines.

The mousepox paper was criticized when it appeared as providing a how-to guide for terrorists; after the anthrax attacks, Atlas recalls, its publication was attacked as a huge mistake. And in Congress, according to *Science* magazine, eight Republicans criticized the poliovirus publication as a "blueprint that could conceivably enable terrorists to inexpensively create human pathogens," and they called on journal editors to take greater care in what they published. Officials in the Bush administration reportedly suggested that biologists employ the practice adopted by cryptographers—voluntary submission of possibly sensitive papers to sponsoring government agencies prior to publication. Some observers note that academic scientists are already willing to accept restrictions on publication imposed by industrial sponsors. Why not concede to restrictions from government sponsors?

To many, the idea seems impractical. In contrast to, say, the *Journal of Cryptology*, which publishes fewer than 20 papers annually, the 11 journals sponsored by the American Society for Microbiology alone put out 6,000 papers a year. But far more important is the fact that a

Balancing act: The American Society for Microbiology's Ronald Atlas and the president's science advisor John Marburger, shown from left to right before Congress, seek to balance science and security (left). Biotech pioneer Craig Venter says all research can be used for good or ill (right).

good deal of biomedical research is double purpose: it may assist bioterrorism, but it can also help defend against it and serve the needs of civilian and military health. Craig Venter, the former president and spark plug of Celera Genomics, told a reporter, "Some people argue that publishing each genome is like publishing the blueprint to the atomic bomb. But it's also the blueprint for a deterrent and the blueprint for a cure." In an interview with the *Chronicle of Higher Education*, Ariella Rosengard, defending the publication of her paper on the smallpox protein, declared, "We need to galvanize the scientific community to develop safer vaccines and therapies, not make it so difficult that scientists say there are so many restrictions that I'm going to study something else. Because then the terrorists really do win."

The dual use of biomedical research helped block a Bush administration proposal to move the bioterrorism work of the National Institutes of Health into the new U.S. Department of Homeland Security, though the two will collaborate to create a bioterrorism research agenda. But the publication issue still looms large. The American Society for Microbiology's journal editors have sought to develop policies that would serve the purposes of both bioterrorism defense and the eradication of infectious diseases. The key policy, adopted in early 2002, was to vet papers for possible hazards—with the aim of raising any problems with their authors—before sending them out for review. Several authors decided on their own to withhold sections of papers for fear of revealing sensitive information to potential terrorists, appealing to the precedent set in 1940, when a number of nuclear physicists voluntarily established a system to suppress the publication of research on defense-related subjects such as uranium.

But the journal editors soon found themselves fielding complaints that the papers lacked adequate information for replication of the reported experiments. Atlas wanted to ensure completeness in scientific publication, but he understood the need to avoid publishing "cookbooks" for bioterrorism. Besides, he worried that the appearance of such recipes in the journals might provoke a government crackdown. Not sure how to proceed, Atlas prevailed on the National Academy of Sciences to call a meeting where biomedical scientists could discuss the issue with federal security experts.

The meeting, held at the academy on January 9, 2003, revealed, as the president's science advisor John Marburger put it in prepared remarks, that past policies appropriate for security in nuclear physics "do not give adequate guidance for the technology of bioterrorism." The proceedings were cosponsored by the Center for Strategic and International Studies, a Washington, DC, think tank, and they pitted scientists, who on the whole insisted on the freedom to publish—even articles like the mousepox, smallpox, and poliovirus papers—against federal security experts, who considered such research sensitive and its publication downright dangerous. George Poste, the chair of a Department of Defense task force on bioterrorism, insistently told the gathering, "I do not wish to see the coffins of my family, my children and grandchildren, created as a consequence of the utter naïveté, arrogance, and hubris of people who cannot see there is a problem." Gerald Epstein, of the Institute for Defense Analyses, an Alexandria, VA, think tank, wondered how the scientists would like it if a sensitive article were "found in a cave in Afghanistan with sections highlighted in yellow."

If some of the rhetoric sounded inflamed, both sides soberly recognized that the issue involved high stakes—both the nation's security and the possibility of "blanket restrictions on science," to quote John Hamre, a former deputy secretary of defense and now president of the Center for Strategic and International Studies. In a recent conversation, Hamre explained, "If the scientific community doesn't take the lead in dealing with the reality of the bioterrorist threat, the security commu-

COURTESY OF THE HOUSE SCIENCE COMMITTEE (CONGRESS); AP PHOTO/LESLIE E. KOSSOFF (VENTER)

nity will take over and do the job in ways that are likely to be wrong." He added that "no group is better qualified than biologists to figure out what biomedical research might be dangerous to publish." At the meeting itself, Marburger stressed that the government needed the help of biologists in identifying and censoring truly sensitive research results.

In a statement issued after the meeting that made clear their willingness to help, Atlas, Thomas Shenk (his successor-elect at the American Society for Microbiology), several other officers of scientific societies, and the editors of a dozen leading journals, including *Science*, *Nature*, and the *New England Journal of Medicine*, declared that scientific manuscripts must be published in "sufficient detail to permit reproducibility." But they went on to say that editors must be watchful of information that might be dangerous in the wrong hands, and that papers likely to generate more harm than benefit should be changed or not published.

Glossing the policy for me, Atlas said he considered it "a call for integrating ethics" into the criteria for scientific publication, a modification of peer review standards to "take into account protecting the public" as well as the quality of the research. He stressed that the refereeing process is "out of government control and hence not a system for censorship. In the end it will be up to the public to see if that is adequate." A few weeks after the statement was issued, Bruce Alberts, the president of the National Academy of Sciences, remarked to the *Washington Post* that the biomedical community was "on the right track" with the problem of biosecurity. "We need to be on the same team with the security folks instead of in opposition."

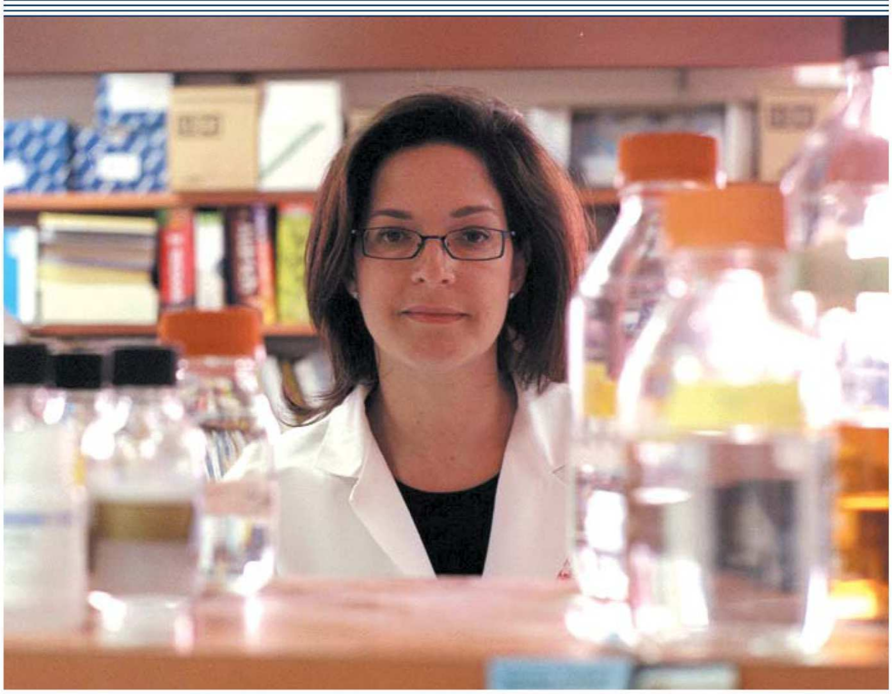
Cooperation, though, runs the risk of co-optation. Early Cold War scientists, eager to protect national security and their influence in federal policymaking, often wound up supporting the government's curtailment of their colleagues' civil liberties. And in any event, the earnest tightrope-walking of U.S. journal editors may well be beside the point. Unlike early Cold War nuclear physics, which was confined to a handful of countries, contemporary biology is a global enterprise. In an unsigned editorial, *The Lancet Infectious Diseases* noted, "No government will really ever be able to control the flow of scientific information. There are 5,000 or more journals in the world, and the Internet is available to anyone who wants to use it."

And locking up lethal biological agents is perhaps as difficult as locking up information about those agents. In the early Cold War, controlling uranium and plutonium was much easier. Raw uranium ore was hard to obtain, and turning it into fissionable fuel involved large, costly processing plants and reactors. But the agents of bioterrorism require comparatively small-scale production plants. Moreover, they are ubiquitous in their natural forms, and new forms—not to mention old ones like the poliovirus—whose DNA sequences are readily available on the Internet can be manufactured using automated tabletop technologies. As Gigi Kwik, a fellow at Johns Hopkins University's Center for Civilian Biodefense Strategies, noted, "You can now finish before lunch projects that used to consume a PhD thesis."

There thus seems little to prevent determined terrorists from obtaining or engineering lethal agents that fall under security restrictions—or from devising new ones. Similarly, keeping foreign doctoral students out of American universities won't necessarily do much to prevent would-be terrorists from acquiring useful technical skills. Universities in Europe and Asia are producing a growing number of science and engineering doctorates and are responsible for half the world's biomedical research. Bruce Alberts told me recently, "None of these efforts to control the weapons of bioterrorism will work without international cooperation. It's really imperative, given how much biology is done outside the United States."

As *TR* went to press, the federal government had not restricted publication of sensitive basic research, but a chill has already fallen over biomedical science. Evident in the constricted flow of foreign students and visitors, as well as in the impairment of some research programs, it is provoking apprehensions that biomedical research and biotechnology could be weakened by the drive for secrecy and security—and weakened without significantly, if at all, limiting the capacities for bioterrorism. TR

"WE NEED TO GALVANIZE THE SCIENTIFIC COMMUNITY TO DEVELOP SAFER VACCINES AND THERAPIES, NOT MAKE IT SO DIFFICULT THAT SCIENTISTS SAY THERE ARE SO MANY RESTRICTIONS THAT I'M GOING TO STUDY SOMETHING ELSE. BECAUSE THEN THE TERRORISTS REALLY DO WIN."



SAL DIMARCO JR./THE NEW YORK TIMES

Resolute: The University of Pennsylvania's Ariella Rosengard published controversial work.

Sense and sensibility: One of Kevin Delin's sensor web pods measures soil and climate conditions in a garden. The gray antennas let it communicate with other pods in a wireless network to relay and process data.

Casting the Wireless Sensor Net

BY GREGORY T. HUANG

PHOTOGRAPHS BY DAVE LAURIDSEN

I DIDN'T KNOW THIS BEFORE, BUT PLANTS HAVE SEX," SAYS KEVIN DELIN. He's gesturing toward two huge cycads, palmlike fugitives from the Dinosaur Age growing in a corner of the Huntington Botanical Gardens, a sanctuary for 15,000 rare plant species in San Marino, CA. Delin's ignorance of botany is excusable. He's an engineer from NASA's nearby Jet Propulsion Laboratory, and what truly interest him are not the male and female cycads but the pair of "sensor web pods" lodged in the ground under the plants. Each pod is the size of a handheld computer and contains a processor, battery, solar cell, radio, memory, and sensors to monitor heat, humidity, and soil moisture. The pods are the surrogate eyes, ears, and even brains of the garden's curators, keeping track of how much sunlight and rain the plants are getting—critical factors for cycads, which need specific conditions to reproduce.

Sensors are nothing new. A car, for instance, uses dozens of them to monitor factors such as engine conditions. But the sensors in today's automobiles, factories, and office buildings are, for the most part, dumb. They lack the intelligence to analyze or act on their findings; instead, they send measurements back to a central processor. Most current sensors are also stuck in place, with any move requiring expensive rewiring. Delin's pods are different. They talk wirelessly with each other and with 18 other pods in the garden, forming their own intelligent network. Every few minutes, the pods update each other about their latest readings, together process the information into an overall picture of temperature and soil conditions, and send this analysis to the curators. It's as if an autonomous, highly aware computer were spread across 40 hectares of landscape.

"It's all about synthesizing global knowledge from raw data on the fly," says Delin. His pods foretoken a future where smart sensors suck in vast amounts of vital data—say, mechanical stresses on the beams of a bridge, or the rumble of an enemy convoy on a moonless desert night—that currently go unrecorded. Wireless and battery-powered, such sensors will be accessed remotely and put where it would be impractical to string data and power lines. Small and cheap, they will be liberally distributed and closely spaced, yielding fine-grained pictures of phenomena such as climate that are currently charted only on a large scale. And because they will act cooperatively—organizing themselves and sharing computations across the mesh—they will provide people with usable chunks of predigested information rather than a confusing wash of numbers.

> A WIRELESS MESH OF SENSING AND COMPUTING DEVICES WILL TRANSFORM THE WAY WE MANAGE OUR HOMES, FACTORIES, AND ENVIRONMENT.

Indeed, wireless sensor networks are one of the first real-world examples of "pervasive" computing, the notion that small, smart, and cheap sensing and computing devices will eventually permeate the environment. That notion has been percolating in information technology circles for more than a decade. But now, after several years of research investments by the U.S. Defense Advanced Research Projects Agency, the National Science Foundation, and a handful of high-tech giants like Intel, the hardware and software fundamental to pervasive computing are emerging.

Though the technology is still in its early days, the range of potential applications is mind-boggling. Scientists at Intel and the University of California, Berkeley, have developed a wireless, pager-sized "chassis" that can be customized with many kinds of sensors. The researchers are using the devices to track microclimates and pests in vineyards, monitor the nesting habits of rare sea birds, and control heating and ventilation systems. And 600 kilometers down the road at the University of California, Los Angeles, other researchers are deploying wireless sensors to gain detailed measurements of the effects of seismic waves on buildings. Still others are working on ways to let businesses monitor and control their work spaces, from local offices to assembly lines half a continent away. "The applications are *everywhere*," says David Culler, a leading networked-sensing researcher at UC Berkeley.

In the minds of many, it's a technology that could prove as important as the Internet: for just as the Internet allows computers to tap digital information no matter where it's stored, sensor networks will expand people's ability to remotely interact with the physical world. Culler calls the devices "a new class of computer systems," distinguished from the hardware of the past by their ubiquity and their collective analytical skill. Within this decade, he predicts, distributed sensing and computing will creep into every home, building, office, factory, car, street, and farm.

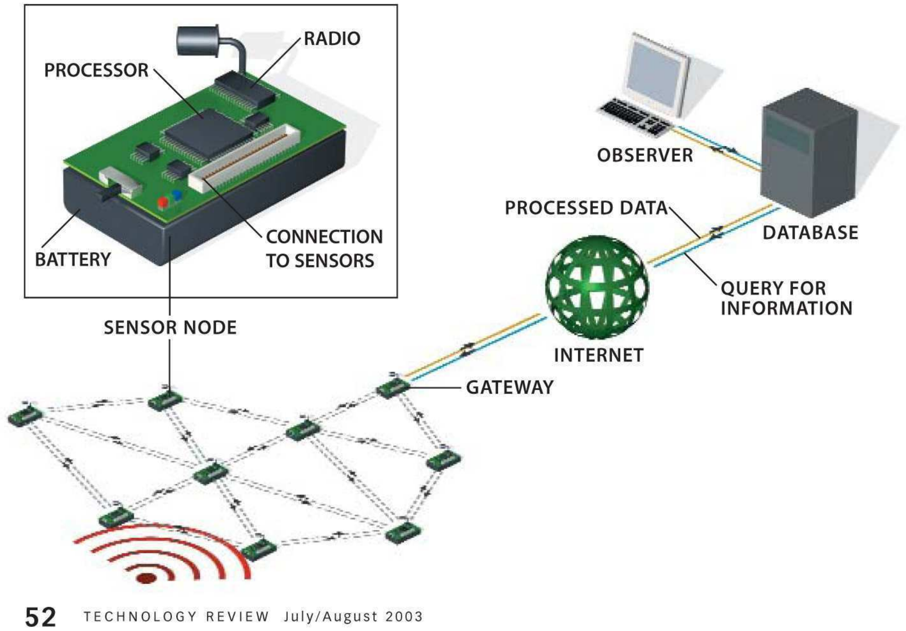
Not surprisingly, there are plenty of challenges before that happens. In many ways, wireless sensor webs are as far along as the Internet was in the 1970s, when the network linked fewer than 200 universities and military labs, and researchers were still experimenting with communications protocols and address schemes. Today, most wireless sensor networks connect fewer than 100 points, or "nodes"; any more and the lines of communication become so tangled that they break down. The cost of the average node is close to $100, while battery life is measured in, at best, months. And no one is exactly sure what application will transform the technology into a commercial bonanza. "Everyone and their aunt and uncle is interested," says Deborah Estrin, director of UCLA's Center for Embedded Networked Sensing. "But it's a struggle to find the business model."

Researchers say none of these problems is likely to be prohibitive. Some wireless sensors are already on the market, and products with intriguing new capabilities could be available within a few years. Sensoria in San Diego, for one, is developing sensors that could turn cars into traveling nodes in urban wireless networks, allowing groups of vehicles to automatically assemble real-time pictures of local traffic or to share communications duties when accessing information about local destinations. William Kaiser, a UCLA electrical engineer and founder of Sensoria, maintains, "The Internet changed how we do business with computers. This will change the way we live our everyday lives."

"THE INTERNET CHANGED HOW WE DO BUSINESS WITH COMPUTERS. THIS WILL CHANGE THE WAY WE LIVE OUR EVERYDAY LIVES."

Anatomy of a Wireless Sensor Net

An environmental disturbance (red) is sensed by nodes in the network. They send radio signals to one another (dashed lines) and process the data—predicting, say, the spread of toxic chemicals or seismic waves. A human observer can remotely access the crucial information.



UNWIRING INDUSTRY

Back at the Huntington gardens, Delin enters a conference room bearing an aluminum briefcase, the kind government agents on TV use to carry top-secret gadgets. He takes out four of his latest sensor pods and pries the cover off of one; underneath are circuit boards holding the pod's guts, including the microprocessor and the radio transceiver that lets it communicate with its companions. He spreads the pods around the room, and within seconds they locate one another and self-organize into a wireless network that monitors temperature and humidity, among other things. A nearby pod—though any of them would do—forwards information from the network to Delin's laptop for display. To show how the network reacts to its environment, Delin disconnects one of the devices. The laptop screen shows the remaining pods compensating by routing data around the missing pod. He attaches an electric fan to one pod, then holds another pod in his hand; the network detects Delin's body heat and switches on the fan.

The pods' ability to communicate by radio, Delin explains, means that they can be scattered in areas that phone and power lines don't reach and moved around at will. But to get data flowing, nodes must find their neighbors automatically and set up radio connections. Those connections can change rapidly, says Delin, so sharing data over the network is a juggling act. Software running

Factory net: A solar-powered Xsilogy node (yellow) receives data from a water-pump sensor (inset) and beams it to the network.

COURTESY OF XSILOGY

on all of the pods coordinates which of them talk to one another and when. The sensor nodes "listen" for one another and set up times to share data, while a network clock keeps the nodes in sync. The network resembles a mesh rather than the hub-and-spoke arrangement used for cell phones; instead of linking each sensor directly to a central communication point, the nodes send data only to neighbors within radio range, saving power.

It sounds complicated, and it is. But decentralized wireless networks like Delin's are already cost effective for heavy industry: Ember in Boston, MA, has sold similar technology to customers frustrated with the conventional wired sensors in their manufacturing or heating and ventilation equipment. One customer used to line the pipes of its treatment plant—where oil and gas are separated from wastewater—with expensive wired temperature sensors, attached to heaters that keep the fluid inside from becoming too thick. If a sensor malfunctioned, a tank could burst, forcing the plant to shut down at a cost of $100,000 per hour, says Robert Poor, Ember's cofounder and chief technology officer. With a wireless network, more sensors can be installed at an affordable price, offering redundancy and yielding more reliable information. "Silicon is cheap. Wiring is not," Poor says.

Several remaining problems, however, obstruct broad commercial application of the technology. The first is its high power consumption. The periodic talk back and forth between the nodes, in particular, is a drain on batteries. "Every bit transmitted brings a sensor node one moment closer to death," says Greg Pottie, a Sensoria cofounder.

A related issue is that sensor nodes' radios have a limited range, usually in the tens of meters. So networking a bigger space—say, a large factory—takes a lot of nodes. Numerous nodes sending lots of data create opportunities for localized failures that could leave parts of the network isolated, says Rick Kriss, CEO of San Diego-based Xsilogy. "There's no such thing as a reliable network, unless you do very aggressive network management," Kriss says. So Xsilogy's nodes periodically broadcast their status, letting the network know if their batteries are running low or their reception is fading. Then the network can compensate by routing around the failure points and alerting the user to impending problems.

High-wireless act: Networked sensors on the ceiling of Deborah Estrin's UCLA lab monitor heat, light, and motion. The researchers are testing ways to process and route data efficiently.

But there's another problem that is harder to work around, and that's price. In a process that is the very opposite of mass production, most sensor-net makers still cobble together off-the-shelf parts by hand, raising the cost of each node into the $80 to $100 range. That price needs to drop below $20 in order for sensor nets to take off commercially, says David Tennenhouse, director of research at Intel.

Standardization could help. "Having open standards and many disinterested groups testing competing approaches will absolutely make or break whether this becomes widely used," says UC Berkeley's Culler. But with so many companies and university labs developing their own prototypes, design standards for wireless sensors and networking protocols are only beginning to emerge. One potentially dominant design is called a "mote"; its operating system, TinyOS, was developed by Culler's group at Berkeley and is undergoing further refinements at Intel and Crossbow Technology in San Jose, CA. The Berkeley motes, which have been tested by hundreds of research groups around the world, are smaller and use less power than most commercial wireless sensors. The trade-off is that they can't process as much data. But many researchers say their adaptability—it's easy to snap on sensors for light, sound, temperature, or movement, say—makes them the networked-sensor world's equivalent of a Windows PC.

In fact, the eventual choice of a wireless-sensor platform could be just as consequential as the emergence of Windows as the dominant consumer operating system—or even, in the eyes of one expert, as the standardization of electricity. "It is sort of like the historic battle between AC and DC," says Larry Smarr, director of the California Institute for Telecommunications and Information Technology in San Diego. "Until there was a ubiquitous winner, the electrical-appliance industry couldn't take off."

A SENSOR NETWORK SHOULD SEND ONLY ITS ANALYSES, NOT THE RAW BITS THEMSELVES. USERS "WANT ANSWERS, NOT NUMBERS."

DIVIDE AND CONQUER

As if ready to take off themselves, 50-odd butterfly-sized motes cling to the ceiling and walls of Deborah Estrin's lab at UCLA, monitoring temperature, light, and motion. Others lie dismantled on desktops and benches. A few of the motes even have wheels; they roll across the floor under their own propulsion, practicing for a day when they'll move around to find the best radio reception or deliver a battery recharge to a failing neighbor. "Here's a picture of the connectivity," says Estrin, holding up a sheet of paper with an incomprehensible tangle of lines on it. It looks like a plate of spaghetti: the number of communication pathways explodes as more nodes are added, making the network more and more crash-prone.

The solution being tested in Estrin's lab: divide and conquer. Think of it as organizing a big dinner party, she says. Meaningful conversations can't occur unless people take turns speaking and listening. And high-level communication is most efficient if people organize themselves into clusters and elect an individual to speak for each cluster. Therefore the nodes cluster themselves and adjust on the fly, changing clusters opportunistically to optimize both power consumption and the flow of information through the network.

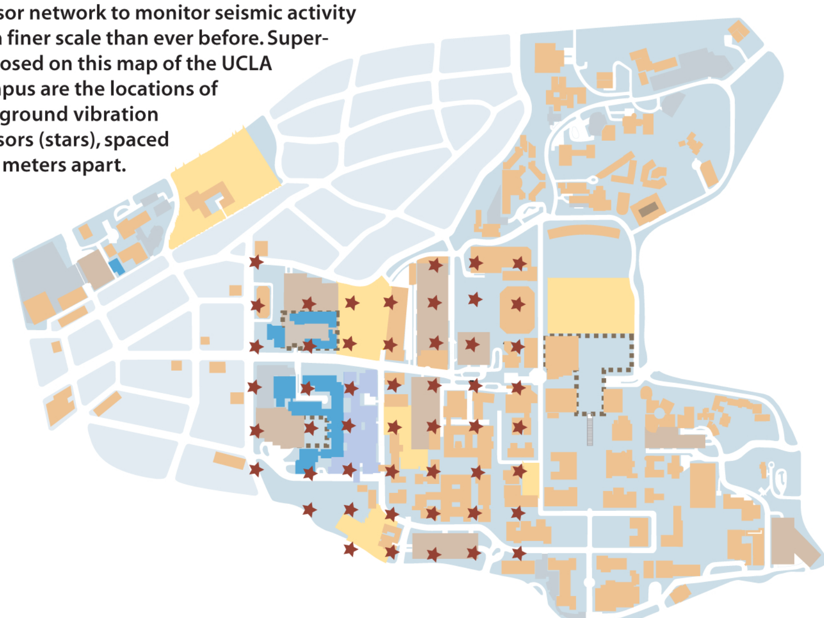
The next challenge is simply how to channel the flood of data. The idea is to put processing into each node, allowing it to condense raw data into patterns and pass along fewer bits than it received. The motes above Estrin's head, for example, could follow her movements and alert their neighbors, which figure out the direction she's walking and transmit just that information—not the entire record of her movements—to a database on a mother node. This node can recommend that lights be turned off, for example, if it decides that Estrin has left the room and no other people are present. Processing data a little at a time throughout the network, says Estrin, is a first step toward programming the system to help make intelligent decisions. It also saves precious battery power.

To be truly useful, a sensor network should send users only its analyses of interesting events, not the raw bits themselves. "People want answers, not numbers," points out Steven Glaser, a professor of civil and environmental engineering at UC Berkeley whose group uses sensor nets to study seismic activity.

Among the answers that engineers and seismologists like Glaser want: how do earthquakes affect individual components of buildings, and how do structures respond to localized variations in an earthquake's strength? A UCLA team led by Paul Davis, a geophysicist and principal investigator at Estrin's center,

Seismic Sensing

Researchers at UCLA are deploying a 50-node sensor network to monitor seismic activity on a finer scale than ever before. Superimposed on this map of the UCLA campus are the locations of the ground vibration sensors (stars), spaced 100 meters apart.



COURTESY OF PAUL DAVIS AND ALLEN HUSKER (MAP)

is deploying a 50-node array of seismic sensors across the campus in an attempt to learn part of the answer. The first step is just to accumulate the data, recorded from the ground at 100-meter intervals—a much higher resolution than that provided by current seismic sensors, which are spaced kilometers apart, says Davis. The researchers will then compare how the ground shakes to vibrations measured at the same time inside a campus building wired by the U.S. Geological Survey after the Northridge, CA, quake of 1994.

The goal is to develop a model of how fine-scale seismic activity affects different structures. Such a model—programmed into portable sensor nets that could be deployed temporarily in city neighborhoods—could help urban planners learn where geological conditions tend to magnify quakes and how to make buildings in those areas safer. In the future, sensors placed near fault lines could even detect approaching seismic waves and trigger alarms, giving building occupants precious seconds to get to safer areas. But, Davis says, "That's blue-sky stuff."

TRANSLATING TODAY'S SENSOR-NET RESEARCH INTO PRODUCTS MAY SIGNIFY A MERGER BETWEEN THE VIRTUAL AND PHYSICAL WORLDS.

GOOGLE FOR THE PHYSICAL WORLD

Smart, autonomous, and self-aware: that's the ultimate vision for sensor nets. In many ways, it *is* blue-sky. But two industry projects provide glimpses of a networked future.

There is a danger that accessing the data collected by sensor networks will be like "drinking from a fire hose, only worse," says Feng Zhao, manager of the Embedded Collaborative Computing research area at the Palo Alto Research Center in California. In other words, being inundated with too much data can be just as paralyzing as not having enough. It's a dilemma that anyone using the Web is well aware of. And, says Zhao, the solution for sensor networks may be similar. In an effort to construct user-friendly interfaces for sensor networks, Zhao's group is experimenting with a new breed of search engine that he describes as "like Google for the physical world."

Imagine, Zhao explains, logging onto the Internet and typing in, "Does my lawn need more water?" The network would translate the question into a standardized database query, examine figures from moisture sensors around your home, and send back a prompt yes or no. Similar systems for supply chain management and security could be available in five to seven years, says Zhao. At warehouses, managers could quiz shelf-mounted sensors about inventory trends, while guards in secure facilities could program smart networks of motion sensors to sound alarms when they notice suspicious patterns of movement.

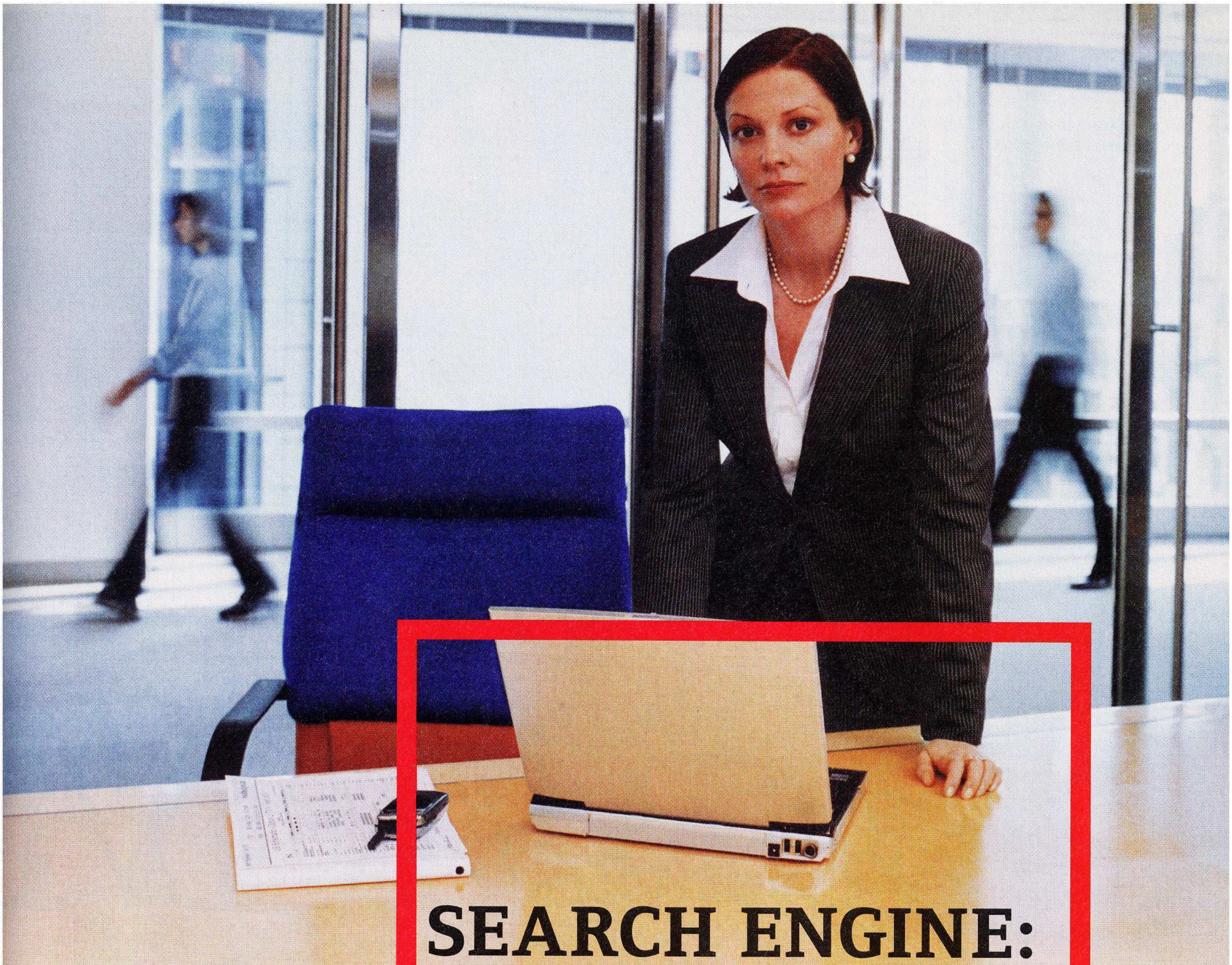
Eventually, sensor nets may even seem alive. At a U.S. Army base in Fort Leonard Wood, MO, this April, Sensoria engineers demonstrated a disturbingly self-aware system that physically rearranges itself in response to changing conditions. As 80 spectators watched, an M1-A1 Abrams battle tank rumbled across a field with a plow attached to its front, blazing a trail through a thicket of unarmed, 12-centimeter-diameter mines. After the tank crushed a half-dozen or so of the mines and proceeded on its way, the remaining mines redistributed themselves to fill the gap behind the tank—hopping through the air with firecracker pops emanating from tiny rocket boosters.

The mines accomplished this feat by emitting and listening for acoustic pulses that helped them locate their neighbors to within a few centimeters, says Kaiser. A disturbance in the network prompts the mines to figure out which neighbors have been moved or destroyed and calculate how to redistribute themselves. On a real battlefield, such smart mines could defeat enemy mine-clearing efforts, or even move out of the way for friendly forces and then reestablish defenses behind them.

Despite such dramatic demonstrations of the power of wireless sensor nets, it's hard to predict whether defense, manufacturing, or some as-yet-unknown field will play host to their killer app. "It's like PCs in the early 1980s. People thought they would be used mainly to balance checkbooks," says Delin. As for the near-term commercial market, it will be a "delectably messy environment for a while," with plenty of opportunity for newcomers, predicts Ember's Poor. That's because the potential applications are all around us—anywhere useful information can be extracted from our environment. When today's research is translated into inexpensive, crashproof products, it may signify nothing short of a merger between the virtual world and the physical world. "It's going to happen," says Zhao. "The question is, how soon?"

Sensing the Potential

COMPANY	TECHNOLOGY	APPLICATIONS
Crossbow Technology (San Jose, CA)	Modular motes with interchangeable sensors	Environmental monitoring, security
Dust (Berkeley, CA)	Four-square-millimeter motes	Inventory tracking, surveillance
Ember (Boston, MA)	Self-organizing nodes and software	Building and factory automation, defense
Intel (Santa Clara, CA)	Modular motes with interchangeable sensors	Monitoring of farm, wildlife, and manufacturing sites
Millennial Net (Cambridge, MA)	Dime-size, low-power nodes and software	Building automation, meter reading, supply chain management
Sensicast Systems (Needham, MA)	Mesh-networking software for sensors	Museum security, landscaping, horticulture
Sensoria (San Diego, CA)	High-performance nodes and software	Defense networks, automotive and health-care systems
Xsilogy (San Diego, CA)	Radios, sensors, and networking software	Industrial and equipment monitoring, heating and ventilation

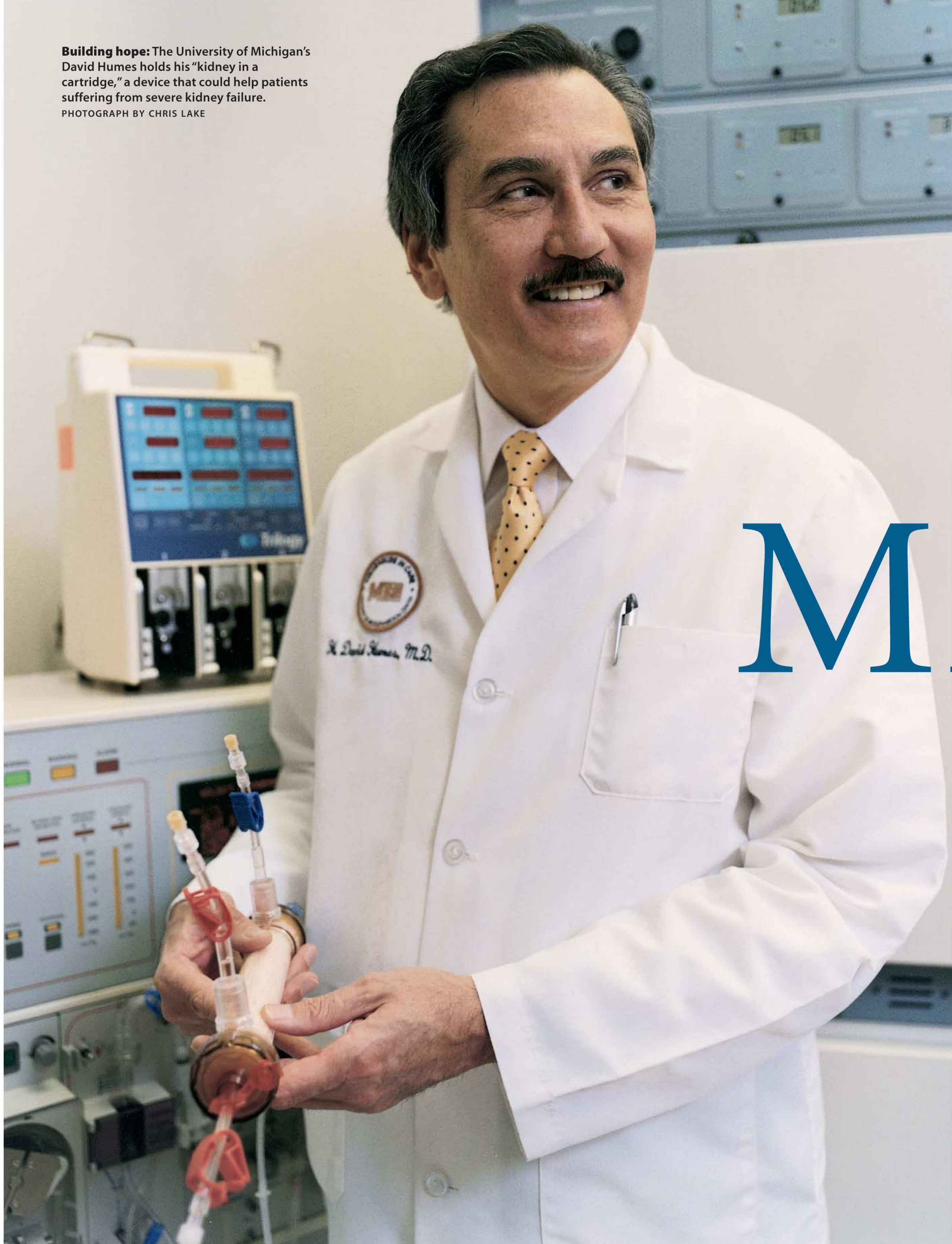


SEARCH ENGINE:

IT consultant who actually finds ways to make you money.

That new system was going to save you money. Only it wound up costing you. Big time. That's when you call in Novell. Our Ngage℠ services provide you with IT consultants who have real-world experience. They don't go around ripping and replacing. They just find ways to make what you have work. And make you money doing it. If you'd like them to apply their expertise for your company, give us a call at 1-800-721-2800 or visit http://www.novell.com/ngage. ➔ WE SPEAK YOUR LANGUAGE.

Novell.



Building hope: The University of Michigan's David Humes holds his "kidney in a cartridge," a device that could help patients suffering from severe kidney failure.
PHOTOGRAPH BY CHRIS LAKE

SAVING LIVES *with* LIVING MACHINES

For many patients with organ failure, artificial devices like dialysis machines are just not enough. Now doctors are combining the unique properties of human cells with man-made materials to create bioartificial organs, including kidneys and livers, that could save thousands.

Around a hospital's intensive-care unit it is often called the spiral of death. Chemotherapy or an infection knocks a patient's kidneys out of service, and within a day or two, inflammation spreads throughout his or her blood vessels. Blood pressure crashes, starving the body of oxygen, and in short order the lungs, liver, and other organs begin to fail. Replacing the kidney's most basic function by using conventional dialysis to clear urea and other wastes from the blood is of little help. More than half of those caught in the grip of acute kidney failure die.

But in a small clinical trial completed last winter, a novel treatment offered the first real hope for patients in acute kidney failure. Six out of the 10 critically ill patients beat the odds and survived; all but one had been judged to have no more than a 10 to 20 percent chance of living.

What appears to have saved them is a plastic cartridge the size of a pair of stacked soda cans containing an unconventional active ingredient: one billion human kidney cells thriving inside 4,000 translucent, hollow, plastic fibers. It's called a bioartificial kidney. Developed after a decade of research by University of Michigan internist David Humes, this hybrid of living cells and artificial structure is at the forefront of a pragmatic effort to find an effective treatment for people whose organs have failed. Though the research may not be as glamorous as attempts to develop an all-artificial heart or other completely synthetic organs, the strategy has a distinct advantage: it seems poised to save lives now. "It's clearly a very promising technology," says William Harmon, a transplant physician at Children's Hospital in Boston and president of the American Society of Transplantation.

BY PETER FAIRLEY

Bioartificial organs' most compelling use may be for kidney failure patients. While a strictly artificial device such as a dialysis machine can cleanse the blood, it can't replace or mimic the subtler metabolic functions of a large, complex organ like the kidney. Dialysis machines just don't do enough to save most patients in acute kidney failure. Nor, in the long term, do they do enough for the hundreds of thousands of people with chronically diseased kidneys. "Patients who are undergoing chronic dialysis become malnourished, and they sort of wither," says Harmon. The solution, believes Humes, lies in harnessing kidney cells themselves—cells that can rapidly react to changes in the body's environment in a way that machines simply can't.

The kidney-in-a-cartridge, which is being developed by Lincoln, RI-based University of Michigan spinoff Nephros Therapeutics, could be ready for widespread use in as little as three years. And it's only one example of the increasingly popular strategy of using living cells to do the heavy lifting in artificial organs. Several academic labs are developing similar devices packed with liver cells to chew up the toxins that accumulate in the blood when the liver suddenly fails. Already in human trials, these bioartificial livers could help patients in acute liver failure, whose only chance today is a rare organ transplant.

While bioartificial organs offer benefits that purely mechanical devices can't match, they still have some severe limitations. For now at least, they are external devices, and the cells inside them stay healthy for no more than a few weeks. Even such temporary support could be a boon for medicine, sustaining thousands of patients and enabling them to regain the function of their own organs or survive until transplant organs become available. But the real revolution will come with the development of permanent, implantable bioartificial organs. That will require new materials that allow the cells to receive nourishment from the body but still protect them from attacks by the recipients' immune systems. Such devices are years from fruition, but Humes and other researchers developing living temporary devices have started laying the groundwork for them—with the potential for eventually saving hundreds of thousands of lives.

Cellular support: Immature kidney cells harvested from donated organs grow in an incubator, waiting to be seeded into bioartificial kidneys. PHOTOGRAPH BY CHRIS LAKE

CELL POWER

Life without properly functioning cells can be hell, and no one knows that better than a dialysis patient. People with chronic kidney disease—400,000 in the United States alone—plug into dialysis machines three to six times a week. The machines pump their blood through permeable tubes, squeezing out plasma (the fluid and proteins making up the bulk of blood) and dissolved wastes, which are tossed out. Then the oxygen-carrying red blood cells and the white blood cells of the immune system are mixed with fresh plasma and returned to the body. Such periodic flushing extends the lives of those with diseased or damaged kidneys, but it doesn't make them healthy. Regardless of age, life expectancy for most patients on dialysis is capped at five years. "There's no question that dialysis in its current mode is an insufficient treatment," says Harmon. Dialysis is even less effective for the more than 120,000 Americans every year whose otherwise healthy kidneys are suddenly knocked out by infection, toxins, or strokes. Even with continuous dialysis, 60 percent of those facing acute kidney failure descend into multiple organ failure and death.

There are few if any options. Transplantation of a healthy, compatible kidney is the only reliable means of escape from dialysis. But those in acute failure are seldom stable enough to endure transplants; and while transplants rescue 14,000 people with chronic kidney disease in the U.S. each year, more than 50,000 languish on waiting lists, thousands of whom die waiting. Meanwhile, a fully artificial replacement for the kidney is unlikely any time soon. Bioengineers lack a complete understanding of what the organ does. And compared to cells, even the most ingenious mechanical device is woefully unsophisticated. "Cell therapy is based upon a billion years of Mother Nature's research and development. We're not that bright," says Humes.

The promise of Humes's bioartificial organ is to deliver the full range of kidney functions, even tasks such as regulating the immune system that are barely understood by medical science. Though the fix is temporary, patients who survive acute kidney failure have a good shot at a normal life, free of dialysis. For patients in chronic failure, cellular support could supplement traditional dialysis, arresting their slide into heart disease and infection, improving their quality of life, and increasing their life span.

Ten years ago Humes was one of the few nephrologists who believed that tem-

porary support with living kidney cells was desirable. He was an early advocate of the theory, now gaining ground, that the organ helps to control inflammation and that the loss of this control is what makes acute kidney failure so deadly. In the early 1990s, Humes made the breakthrough that enabled the bioartificial kidney: he found a source of cells. Humes discovered how to isolate the immature cells that form the kidney's tubules—its functional center. Within a few years, he had figured out how to coax these cells to form mature tubule structures in the lab.

To make the devices that Humes and Nephros are testing, technicians harvest immature kidney cells from donor organs deemed unsuitable for transplantation and seed them into hollow, plastic fibers *(see "Bioartificial Treatment," this page)*. There the cells multiply and organize to form a continuous blanket of tissue just one cell thick, transforming each fiber into a living, working kidney tubule. "It's basically what you would see in a kidney," says Humes. "It's their natural architecture."

The first human tests showed that Humes's kidney is safe. What is more exciting is that the device also appeared to pull a few of its first patients out of acute kidney failure, even though the U.S. Food and Drug Administration limited treatments in this initial trial to 24 hours. How such brief support from living tubules could save someone in such desperate condition isn't clear. Humes believes that among the substances that the tubule cells add to blood are molecular signals that instruct the patient's immune system to reign in the inflammation ravaging blood vessels throughout the body. By smothering this inflammatory "forest fire," suggests Humes, the tubule cells stabilize blood pressure, oxygenating and rejuvenating the patient's organs. "We view this treatment as almost like a drenching rain for 24 hours," he says.

LIVING LIVERS

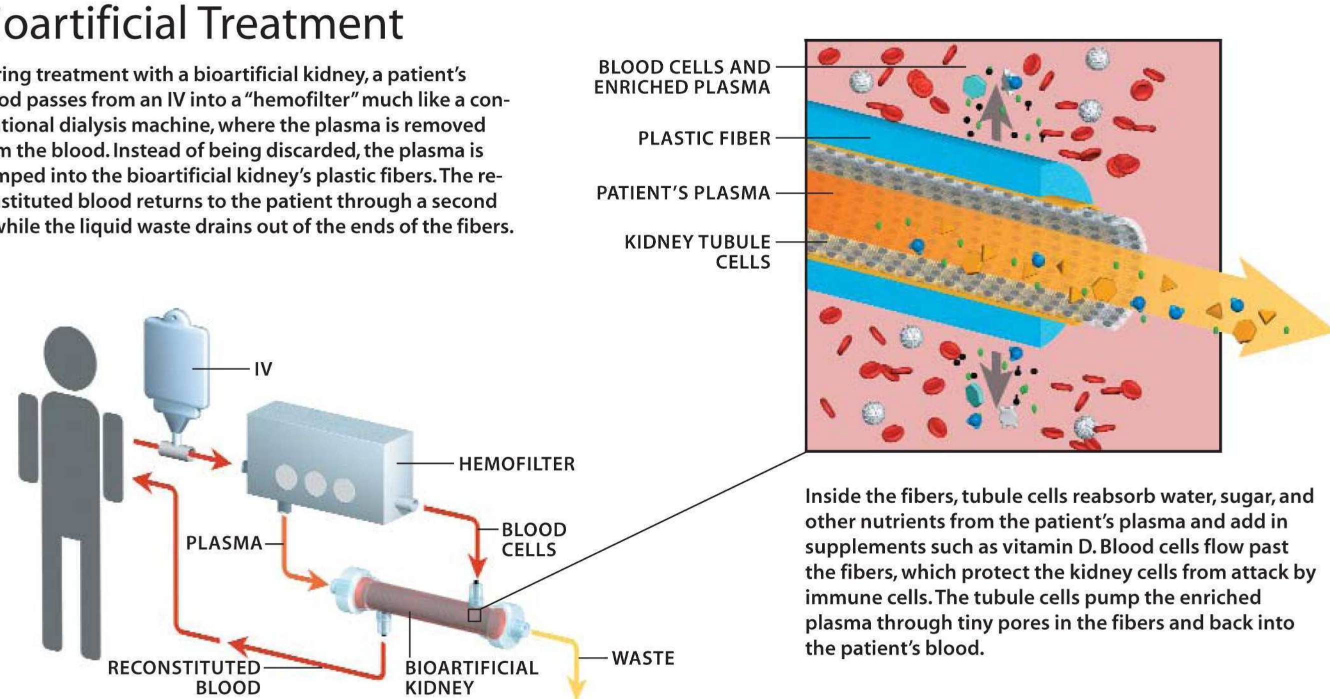
Humes's success is raising hope among corporate and academic researchers who are busy developing similar temporary-support devices for patients in acute liver failure, a rarer yet even more deadly condition. An acute case of hepatitis or a chemical assault (most commonly an overdose of the pain reliever acetaminophen) causes acute failure in about 2,000 people in the United States each year. Without transplants, nearly 80 percent will die, as ammonia and other toxins in the blood degrade the blood-brain barrier, causing the brain to swell out of control. Liver-assist devices analogous to Humes's bioartificial kidney are already in advanced human tests, but despite years of development, definitive success has been elusive.

Bioartificial livers employ a cartridge full of liver cells to break down toxins in blood plasma fed into hollow plastic fibers. By taking over liver function, these devices could allow patients' ailing organs to recover—or at least support them until transplant organs become available. George Mazariegos, a transplant surgeon at the University of Pittsburgh's Thomas E. Starzl Transplantation Institute believes such devices might one day do more than carry patients through the most acute phase of liver failure; he hopes that by continuing to support patients for several weeks, bioartificial livers will enable an increasing number to recover the function of their own livers, avoiding the ordeal of transplantation and freeing up donor organs for those in greater need. "Cell-based therapies are going to be part of the mix, for sure," he says.

Finding the right cells may be the key to success. The earliest bioartificial-liver devices used liver cells from pigs to detoxify blood, but concerns over the possible transfer of porcine viruses to humans—unlikely as many researchers considered it to be—frightened investors and dried up financing for these projects. In March, investors pulled the plug on yet another bioartificial-liver company. San Diego-based Vitagen was in advanced clinical trials with a device employing cells cultured from a human liver tumor. These cells had been "immortalized," meaning they could be multiplied ad infinitum—so they were easy to come by. There are risks attached to using tumor-

Bioartificial Treatment

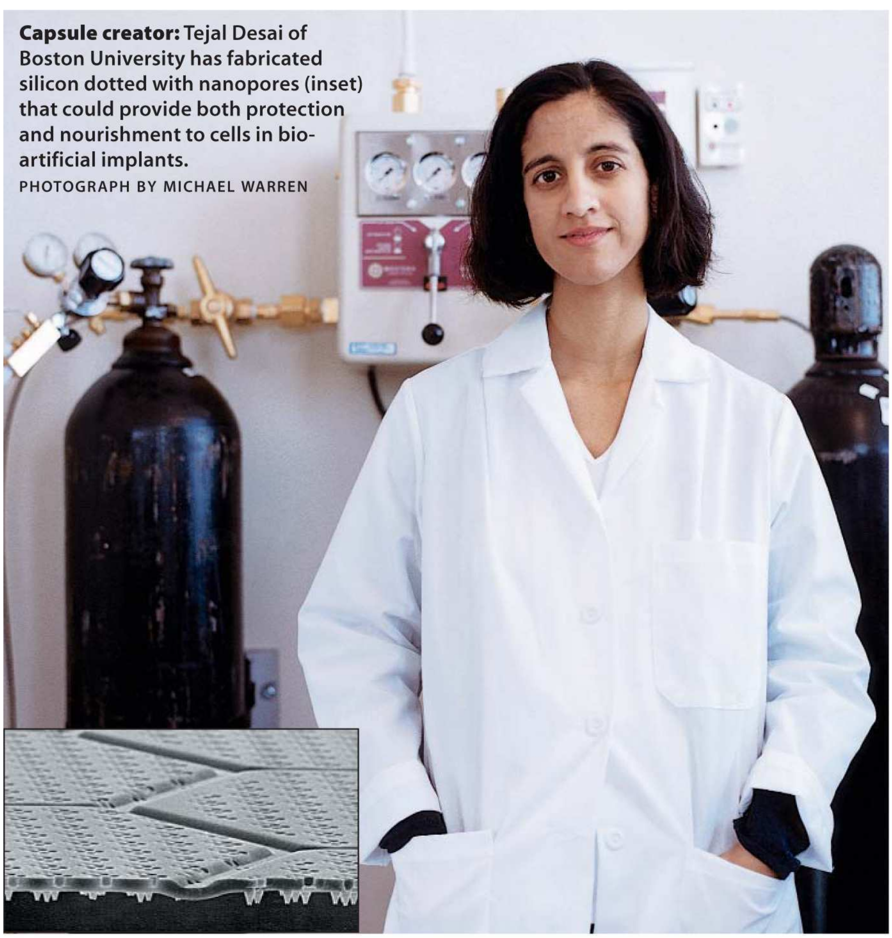
During treatment with a bioartificial kidney, a patient's blood passes from an IV into a "hemofilter" much like a conventional dialysis machine, where the plasma is removed from the blood. Instead of being discarded, the plasma is pumped into the bioartificial kidney's plastic fibers. The reconstituted blood returns to the patient through a second IV while the liquid waste drains out of the ends of the fibers.



Inside the fibers, tubule cells reabsorb water, sugar, and other nutrients from the patient's plasma and add in supplements such as vitamin D. Blood cells flow past the fibers, which protect the kidney cells from attack by immune cells. The tubule cells pump the enriched plasma through tiny pores in the fibers and back into the patient's blood.

JOHN MACNEILL

Designer liver: In this bioartificial liver created by the University of Pittsburgh's Jörg Gerlach, cells can survive for months.
PHOTOGRAPH BY KAREN MEYERS



Capsule creator: Tejal Desai of Boston University has fabricated silicon dotted with nanopores (inset) that could provide both protection and nourishment to cells in bioartificial implants.
PHOTOGRAPH BY MICHAEL WARREN

derived cells, however, and more significantly, the cells had less-than-normal liver function. Nonetheless, the technology was showing promise in trials, which were halted by the company's demise.

Normal human liver cells clearly would be preferable. Immortalized liver cells retain a youthful capacity for growth because they are frozen in an early stage of development, but as a consequence they have not attained some of their most important detoxification tricks. "Immortalized cells are blocked in their ability to mature, so their ability to support patients is minimal," says Lola Reid of the University of North Carolina at Chapel Hill. Reid says that what is needed are young yet normal human cells, akin to Humes's immature kidney cells, that can grow and develop to populate a bioartificial device. To that end, she is developing cell-handling methods to isolate and amplify immature liver cells from donor organs.

Improvements in device design will help deliver more metabolic firepower as well. Jörg Gerlach, who recently moved to the University of Pittsburgh's McGowan Institute for Regenerative Medicine from Berlin's Charité Institute for Transplantation and Organ Regeneration, has developed a bioartificial liver that employs three types of hollow fibers woven through human liver cells harvested from transplant rejects. One set of fibers delivers oxygen to the living cells, keeping them in metabolic overdrive, while the other two pump plasma respectively to and from the cells, a setup that resembles the natural architecture of the liver. "Our cells spontaneously reassemble into tissue structures. Under these circumstances, the human cells survive for more than two months," says Gerlach, who has already initiated human tests of the device in Germany. Larger trials in the United States could begin within a year.

ADVANCING IMPLANTS

But what of the hundreds of thousands of patients with chronically diseased organs? Bioartificial-organ technology could restore their health as well—if it can make the leap from today's temporary, external devices to long-term implants. Success with extracorporeal devices is inevitably stirring hope for bioartificial implants to treat this much

larger need. Though researchers have pursued the idea since at least the 1970s, the field had been all but abandoned after continual disappointment. The problem: researchers couldn't find a way to fully shield the cells inside an implanted device from recipients' immune systems. Studies of encapsulated liver, pancreatic, and kidney cells have all run into problems due to immune rejection.

In fact, the porous plastic fibers that protect the cells in current bioartificial kidneys and livers from assault have failed in implants time and again. Their minute openings can defend against immune cells, but smaller armaments of the immune system, such as antibodies, can still penetrate the implant and, over time, break down its cells. It's not a problem in temporary external devices, but in an implant, the detritus from dying cells passes out to the surrounding tissues, prompting scarring and blood clots. Eventually this seals off the implant, starving the cells still living inside.

Advances in nanotechnology could provide the solution: a material able to handle the seemingly contradictory tasks of isolating the cells from the immune system while allowing them to actively participate in the body's function. Boston University biomedical engineer Tejal Desai believes nanotech can help fashion capsules with pores that can protect implants from even the tiniest immune invaders. "We can achieve absolute control over what gets into the system, what gets out," says Desai.

Desai is developing a bioartificial pancreas that could extend diabetics' lives and free them from pinpricks. She starts with silicon and etches it full of holes with techniques adapted from microchip production. The holes are 12 to 18 nanometers across, a fraction smaller than an antibody molecule. Desai then shapes the porous silicon into a small capsule or disc and fills it with living, human pancreatic cells. Surgically implanted in rats whose pancreases have been destroyed, these silicon capsules have elicited none of the clotting or scarring that doomed earlier implants. Moreover, insulin produced by the implanted cells maintained the rats' blood sugar levels through the two-week test period, sustaining rats that would otherwise have perished in a matter of days. Within a year, Desai hopes to begin tests in large animals (probably dogs) of a prototype implant for diabetics.

William Fissell, a researcher in Humes's University of Michigan lab, believes that similar silicon membranes could be the key to bioartificial kidney implants. But unlike Desai's pancreatic implants, a bioartificial kidney must filter more than 100 liters of fluid each day. That's easy for a large external cartridge with pumps to do, but filtering that much fluid is difficult in a much smaller implant, especially when nanopores constrain the exchange of fluid. The challenge is to design a material whose openings pass liquid efficiently and can support many tubule cells, yet which still protects the cells from antibodies. Fissell is already testing an elegant solution: stretching nanopores into elongated nanoslits with far more efficient fluid dynamics. If these slits can keep the antibodies out and filter fluids using only the body's blood pressure, bioartificial kidney implants might one day replace dialysis for patients with chronic kidney failure.

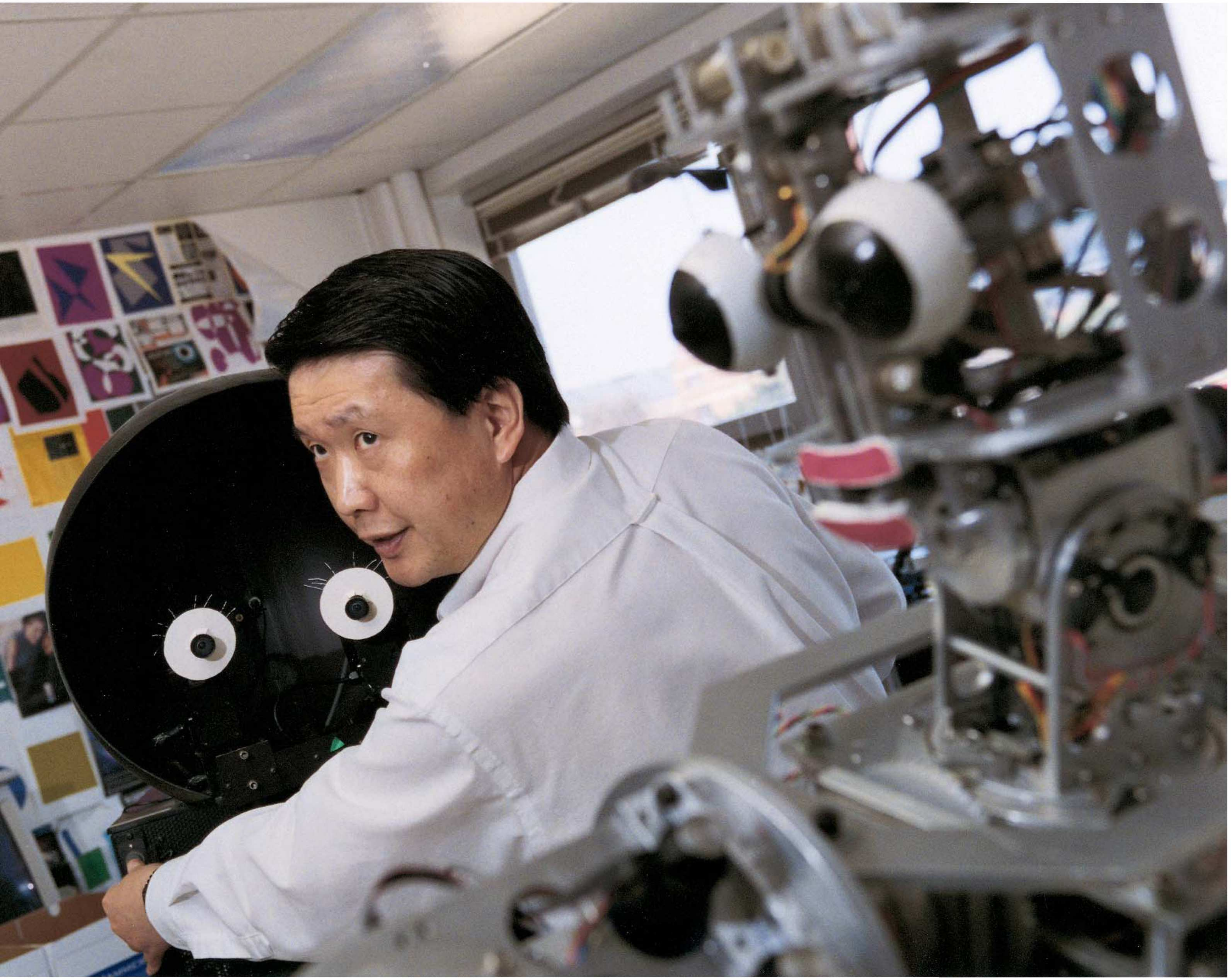
But until then, external devices like the kidney-in-a-cartridge are the best hope. Emil Paganini, a leading dialysis authority at the Cleveland Clinic, is convinced of the bioartificial kidney's potential, and the technology has not disappointed him. Five of Paganini's patients were among the first 10 treated. He vigilantly followed their 24-hour treatment and witnessed consistent improvement. In one case, a patient's response to the treatment astounded even this seasoned physician, who has seen his share of against-the-odds recoveries: the young man's kidneys, poisoned by antifreeze, began to function again while his blood flowed through the bioartificial kidney, then shut off when the device was removed. "That blew my mind," says Paganini. The patient's kidneys eventually rebounded, and today the man is healthy.

After decades of frustrating research on purely artificial organs, such experiences are redefining the possibilities of organ replacement, reviving hopes for the struggling field. As Paganini puts it, "The concept of a bioartificial organ is in and of itself exciting." But what's even more exciting to physicians like him is that bioartificial organs, hybrids of the living and the synthetic, could soon be saving thousands of lives.

Bioartificial Potential

RESEARCH TEAM	DISEASE TARGET	TECHNOLOGY	STATUS
Nephros Therapeutics (Lincoln, RI) and **David Humes, University of Michigan** (Ann Arbor, MI)	Acute and chronic kidney disease	External and implantable bioartificial kidneys	Human trials (external device only)
Jörg Gerlach, University of Pittsburgh (Pittsburgh, PA)	Acute liver failure	Bioartificial liver using natural liver structure	Human trials
Lola Reid, University of North Carolina (Chapel Hill, NC)	Liver disease	Bioartificial liver using normal human liver cells	Prototype
Amaranth Therapeutics (Cambridge, MA) and **Lawrence Rosenberg, McGill University** (Montréal, Québec)	Diabetes	Pancreatic islet cells in bioartificial organs	Raising funds for animal trials
iMEDD (Columbus, OH) and **Tejal Desai, Boston University** (Boston, MA)	Diabetes	Insulin-producing cells in nanoporous silicon implants	Animal trials
MicroIslet (San Diego, CA) and **Daniel Salomon,** the **Scripps Research Institute** (La Jolla, CA)	Diabetes	Insulin-producing cells in porous organic-polymer implants	Animal trials

DEMO



Family portrait: Juyang Weng focuses his attention on SAIL, his first "developmental" robot, while younger brother Dav looks on.

TEACHABLE ROBOTS

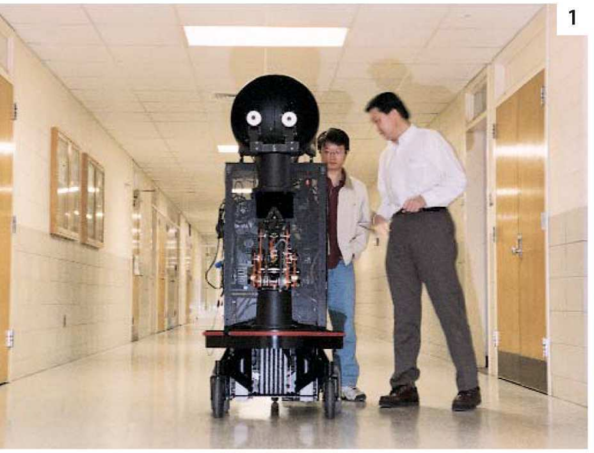
Want the perfect mechanical assistant? Forget about programming, says Juyang Weng. Just take these robots to school.

Like any proud parent, Michigan State University computer scientist Juyang Weng has a lot to say about what sets his little ones apart from their peers. Traditional robots, he explains, must be specially programmed for new tasks. And you just can't teach them much. Sure, they can acquire data—but only within narrowly defined parameters set ahead of time by their programmers. "But human learning is not like that," Weng says. "Human learning is real-time, online, on the fly." And that kind of learning, Weng says, is essential if you want a machine to be able to cope with the unexpected—unpredictable terrain, new people or objects, noisy settings—which will surely confront robotic household assistants and military machines alike.

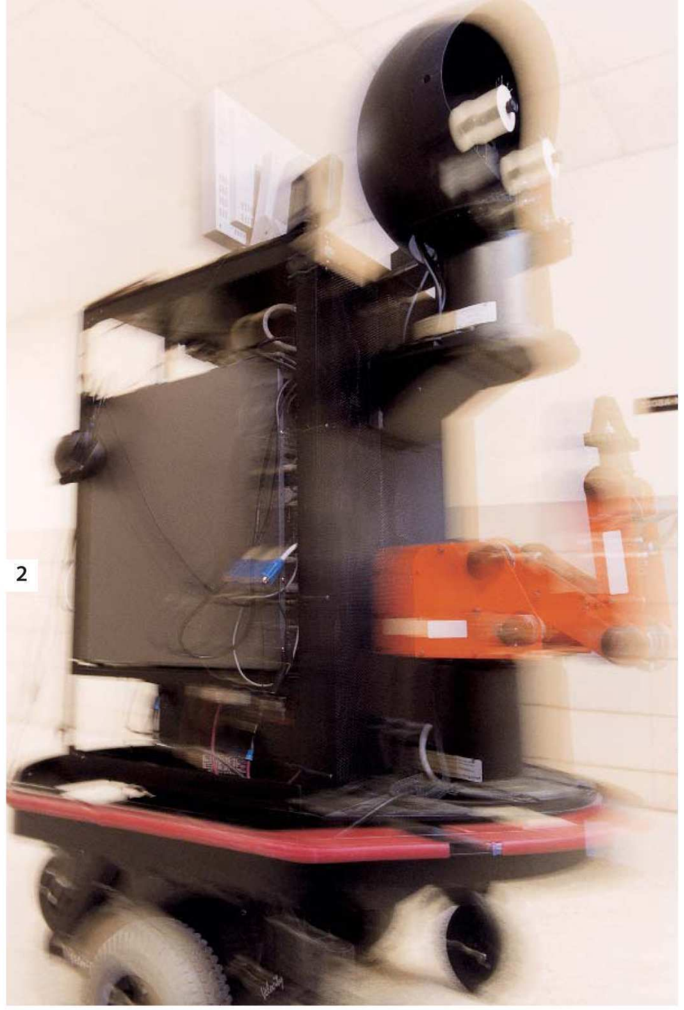
In 1994, Weng and his team set out to build a robot with a capacity for learning like that of a human baby. They came up with a black, moon-faced machine named SAIL, short for Self-Organizing Autonomous Incremental Learner, endowed with what Weng calls a "developmental program"—a program that imparts attributes such as curiosity. Then SAIL was "born." "'Birth' means that the robot starts to interact with the real world, just like a baby interacts with his doctors, his father, his mother," Weng explains. "These interactions make the robot gain a sense of the outside world." Through such exploration, SAIL has learned tasks like navigation, identifying and sorting objects, even some speech. And he now has a younger—though physically more sophisticated—sibling, Dav. Weng introduced his robotic family to *Technology Review* senior editor Rebecca Zacks.

PHOTOGRAPHS BY CHRIS LAKE

1-2. Just like a human child, a developmental robot such as SAIL needs good teachers. To give SAIL a lesson in navigation, for example, Weng and graduate student Xiao Huang walk the robot through the halls of Michigan State's Engineering Building. SAIL's two camera eyes survey the scene, while his human teachers push force sensors on the back of his shoulders to indicate when he should move left or right to turn corners and avoid passersby. Eventually, SAIL gets the idea and can navigate the hallway on his own. "Basically it's like a kid on a bicycle," says Weng. "You hold onto it to practice, and you let it go when it's more skillful."



1

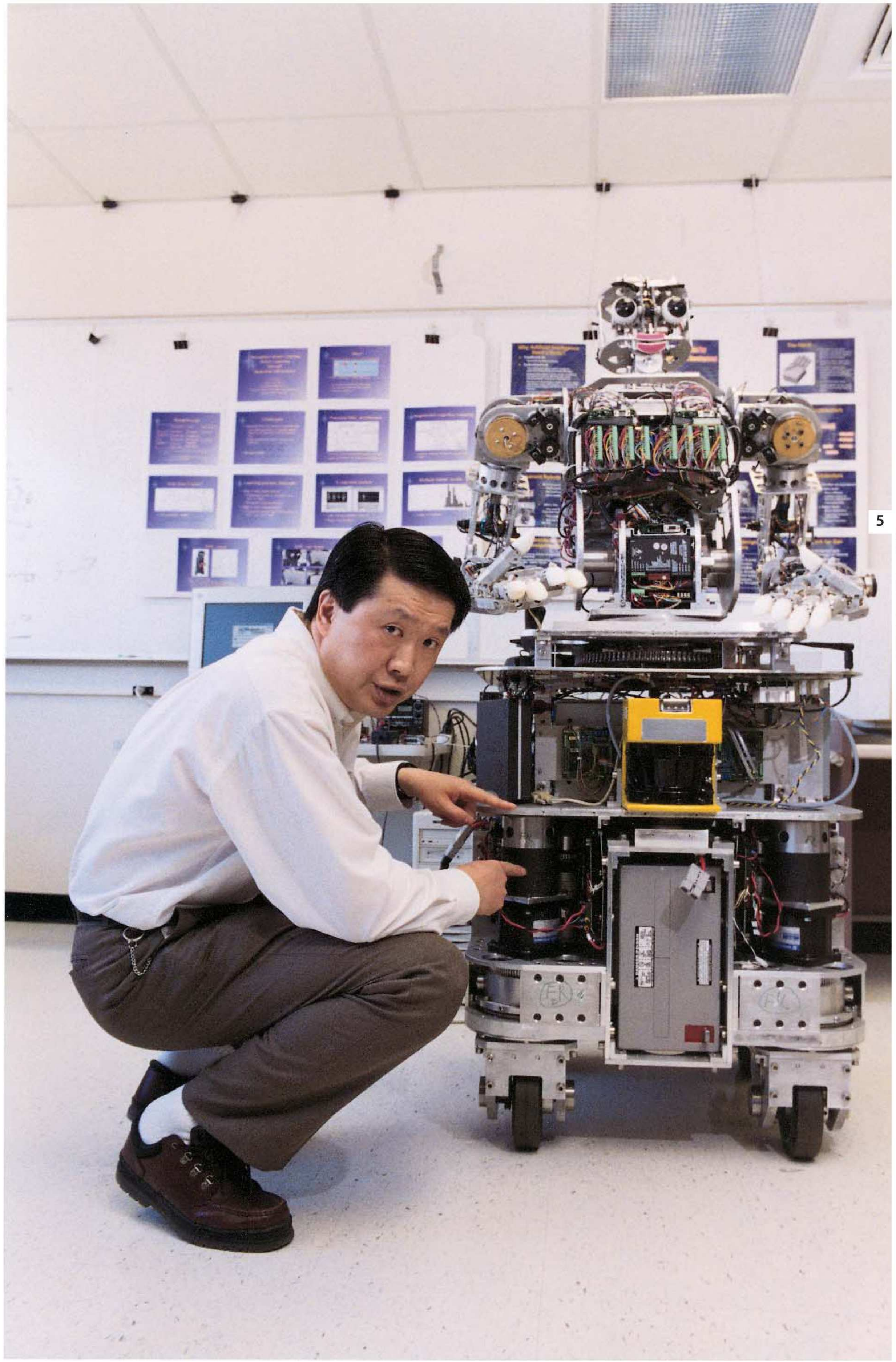


2

3

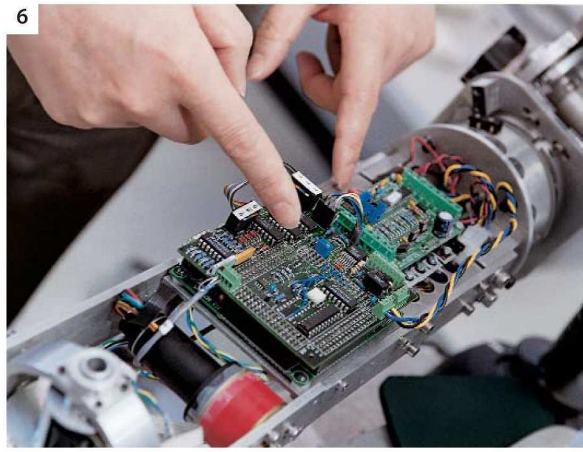
4

3-4. Who says Barbie isn't an educational toy? Weng uses her, along with a host of other dolls and stuffed animals, to teach SAIL to recognize objects. SAIL holds the doll using its orange arm and rotates it to get a look from all different angles. Weng presses small switches on the robot's arm that tell SAIL that the name of this toy is "Barbie," and that its size is small. After just three or four practice runs with a new toy, Weng says, SAIL can tell you the toy's name on its own, using a voice synthesizer to speak it aloud. What's more, the robot can sort the toys he's familiar with by size, dropping them into boxes labeled "small" and "large."



5

5. SAIL's intellect has grown a lot through years of such training exercises, but the robot's body—with its simple sensors and restricted mobility—limits what it can ultimately do. So last year, Weng and his crew put together a new sibling for SAIL, a shinier, more humanoid creature called Dav, pronounced "Dave." Weng explains the name: "It's a kind of a variant form of the word 'development.' We just changed it a little bit, from *e* to *a*." Dav has camera eyes that can pan, microphones for ears, and lips and eyebrows for making basic facial expressions. His multijointed arms and hands are equipped with sensors that register position, force, motion, and other variables. Weng bends down to point out the equipment that drives the machine's wheels. "Each wheel is handled by two motors," he explains, "and the four wheels are synchronized so they don't fight each other."



6

6. Loading Dav up with sensors, effectors, and electronics presented a challenge, Weng says: dealing with all the wires. If each device were connected by its own wire to the central "brain" in Dav's abdomen, he explains, pointing out a sensor in the robot's arm, "you would have a few hundred wires running through the elbow or through the wrist." That would be an unacceptable impediment to the robot's flexibility, so the researchers chose to network all of Dav's embedded devices to save both space and weight. Even with such tricks, Dav weighs in at 242 kilograms.

Despite his size and his mechanical sophistication, Dav is still a baby. Soon, he will start down the trail blazed by his brother SAIL, learning to walk, talk, and eventually, perhaps, understand the world around him to a degree no other robot has achieved before. And as Weng perches between his two offspring, one has to wonder if they both might learn a little bit about sibling rivalry. TR

POINT OF IMPACT

WHERE TECHNOLOGY COLLIDES WITH SOCIETY, BUSINESS, AND PERSONAL LIVES

By Erika Jonietz | Photograph by David Deal

TOTAL INFORMATION OVERLOAD

Robert L. Popp

POSITION: Deputy director, U.S. Defense Advanced Research Projects Agency Information Awareness Office

ISSUE: Terrorism Information Awareness. This DARPA project, formerly known as Total Information Awareness, seeks better technologies to detect terrorist attacks but has roused the ire of privacy advocates.

PERSONAL POINT OF IMPACT: Co–program manager, Terrorism Information Awareness

TECHNOLOGY REVIEW: There have been wildly varying reports about what Terrorism Information Awareness seeks to do. Some groups opposed to the project have said it includes efforts to link public and private databases, with information ranging from consumer buying habits to medical records, into a giant "metabase." Is there any truth to this?

ROBERT POPP: First off, let's talk about what Terrorism Information Awareness, or TIA [TEE-ah], is. It's a visionary R&D program that is developing and integrating a variety of information technologies into a prototype system/network to detect and preempt foreign terrorist attacks. As technologists, we are trying to provide the foreign intelligence, counterintelligence, and counterterrorism communities with prototype information technology that will lead to better collaboration, analysis, and decision-making. If we successfully transition these technologies to the operational agencies, we think government decision-makers will be empowered with knowledge about terrorist planning and preparation activities that will help them make informed decisions to prevent attacks from occurring against the United States.

TR: Will TIA look at U.S. citizens to do any of that?

POPP: No. TIA is not a domestic surveillance capability, nor is any U.S. citizen's privacy changing as a result of TIA. That's one thing that's been widely reported, and nothing could be further from the truth. We are providing operational agencies within the Defense Department and intelligence community with analytical tools that we hope will improve their ability to counter terrorism. These agencies are experimenting with the TIA tools using data and databases they currently have available to them, in accordance with existing laws, regulations, and policies.

TR: So you're not scanning databases.

POPP: Correct. We're not developing technology that will surreptitiously scan or pull data out of a database. TIA is also not creating a grand database of dossiers on U.S. citizens, or developing collections technology to mine transactional or other kinds of data on U.S. citizens that is prohibited by law.

TR: What kinds of information constitute transactional data?

POPP: Examples might be the purchase of airline tickets to potential attack sites for reconnaissance, the purchase of materials for some kind of bomb, different types of communications transactions—

TR: Like this phone conversation, or an e-mail?
POPP: Yes. Phone conversations, e-mails, chat messages, newswire stories, et cetera, are all examples of what we consider to be communications transactions.

TR: Where do you think the false perceptions about your work come from?
POPP: Back in November of 2002, as the Homeland Security Bill was being passed, a national newspaper published a column that asserted the bill would permit DARPA to create a system—TIA—to continuously update electronic dossiers on the transactions of every American. As I said earlier, nothing could be further from the truth. But unfortunately a lot of news outlets and Web sites picked up the story and printed this information as if it were fact.

In retrospect, we could have been—and should have been—more outspoken in the public and with Congress about what we were and were not doing in TIA to straighten out the record. The program's name change is designed to help clear up the confusion, to make it absolutely clear that the goals of TIA are to protect the U.S. and its citizens from foreign terrorist threats, period.

TR: So what are the technologies being developed under TIA?
POPP: In broad terms, the technologies we're focused on are collaboration, analysis, and decision support tools; foreign-language translation; pattern recognition and predictive modeling; databases and privacy protection; and biometrics. We have numerous programs developing these technologies, and TIA is the program that integrates these technologies into a unified network/system.

TR: Are any of these technologies anything like those people have expressed concern over—examining public or private-sector databases, for instance?
POPP: Let me answer this by describing the two threads of activity we're pursuing in TIA, namely, an operational thread and a purely R&D thread. This distinction

is important to understand because it has been a major source of confusion in the public about what we're doing in TIA.

The premise driving the operational thread is a widely held belief that the data necessary to *effectively* counter the terrorism threat is already in government-owned databases. This was certainly one of the conclusions from the joint House-Senate inquiry of the events that led to the failure of 9/11. For example, two of the 19 hijackers were on the State Department/INS watch list; these same two hijackers were also sought by the CIA and FBI as suspected terrorists. The problem is, the data exist in different databases and are managed by different agencies. Within this thread, TIA is essentially doing two things: first, we're building an R&D network to allow agencies to collaborate and experiment with prototype information technology for counterterrorism, and secondly, we're empowering these analysts with a variety of tools enabling better analysis and decision-making.

There is another community of people who believe that all the data necessary to *effectively* counter the terrorism threat is in fact not entirely in government databases; this premise drives the R&D thread. Instead, there may be more information in the greater information space that might prove valuable for the government to exploit in its counterterrorism operations, but currently this data is not used due to legal or policy restrictions. This thread is testing the hypothesis that when terrorist organizations engage in adverse actions against the United States, they make transactions in support of their plans and activities, and those transactions leave a signature in the information space. Those transactions will most likely span government, private, and public databases.

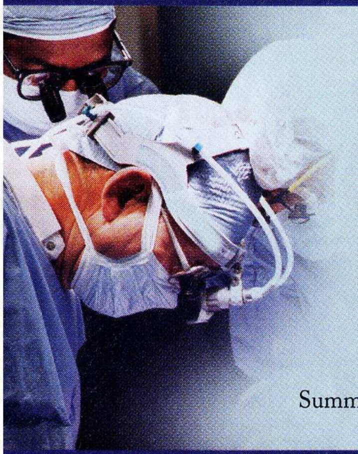
The challenge for TIA here is twofold: First, is the signature detectable when embedded within a world of information noise? Second, in what part of the information space does that signature manifest itself? Ultimately, our goal within this thread is to understand the level of improvement possible in our counterterrorism capabilities if the government were able to access a greater portion of the information space, while at the same time considering the impact—if any—on the right to privacy, and then mitigate this impact with privacy protection technology. If our research does show a significant improvement in the government's ability to predict and preempt terrorism, then it would be up to the policymakers, Congress, and the public at large—not DARPA—to decide whether to change law and policy to permit access to such data. One footnote: because the government today does not typically access some types of transactional data that *may* prove meaningful, all of this research is being done with synthetic, simulated data.

TR: There's quite a bit of public concern over ideas like that, and about technologies TIA is developing like facial recognition that people worry could be used to track them. How valid are those worries?

POPP: All of us know that technology has shaped how hard or easy it can be to invade people's privacy. The government already has plenty of technology right now that could be used to invade people's privacy if used maliciously. But our laws are what control how the technologies may be used and applied and on what information. Our privacy is protected by the law, not the fact that it is technically difficult for the government to quickly make sense out of the information that it already possesses. But this difficulty sorting through government information does make it harder to stop terrorists.

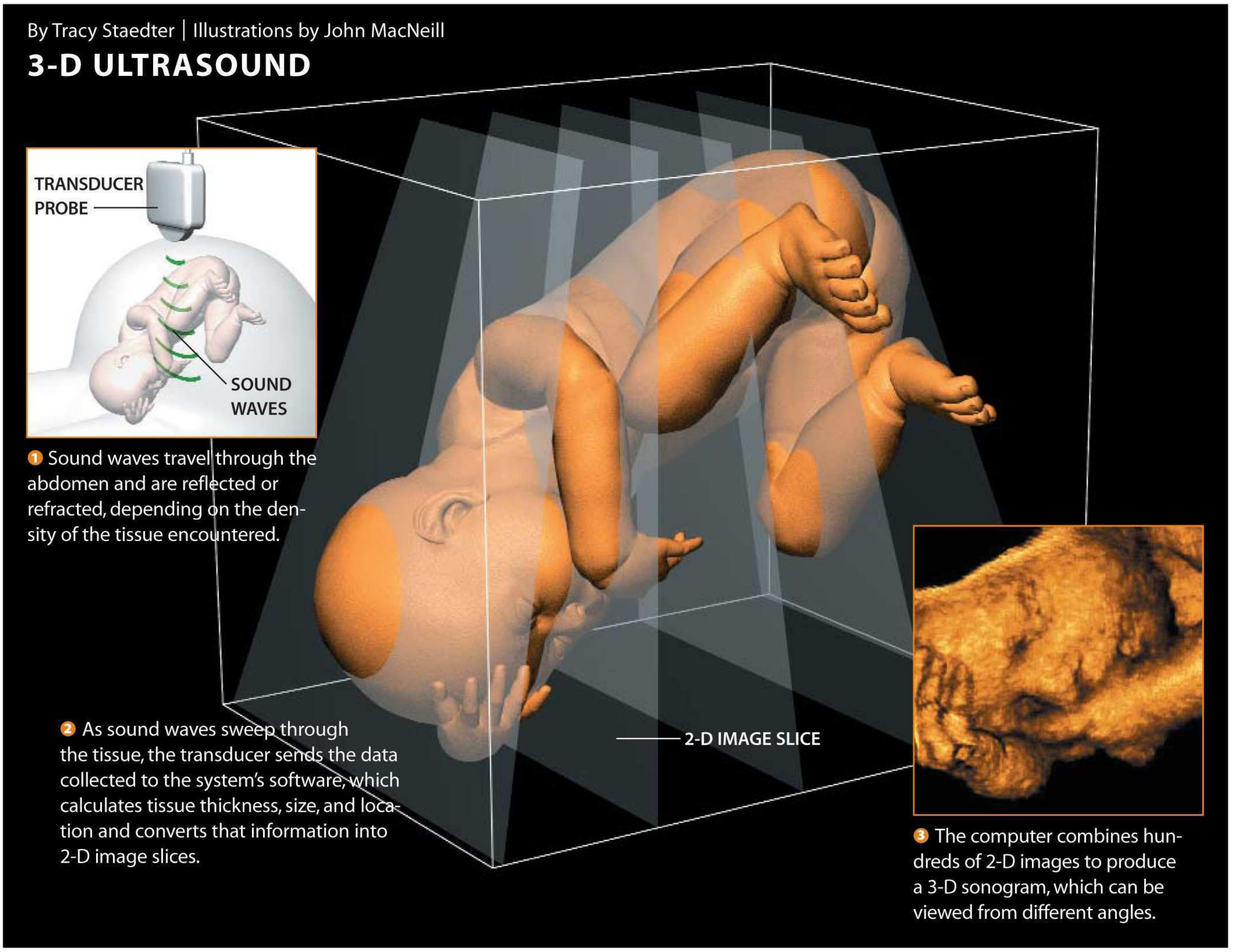
Americans' basic privacy will not change unless Congress changes the law on what information the government may collect and how it may be used. The issue in our view really isn't a matter of technology. The difference between the tools and the rules, what can be done and what *may* be done, is crucial. Does protecting privacy mean we should take away the few rudimentary tools that our agencies in the federal government have now to share data and collaborate—phone, fax, and e-mail? Of course not. Ultimately, what TIA is trying to do is give our counterterrorism agencies far better tools to do their job. TR

For an expanded version of this interview, go to www.technologyreview.com/impact/.



By Tracy Staedter | Illustrations by John MacNeill

3-D ULTRASOUND



❶ Sound waves travel through the abdomen and are reflected or refracted, depending on the density of the tissue encountered.

❷ As sound waves sweep through the tissue, the transducer sends the data collected to the system's software, which calculates tissue thickness, size, and location and converts that information into 2-D image slices.

❸ The computer combines hundreds of 2-D images to produce a 3-D sonogram, which can be viewed from different angles.

SOURCE: AARON FENSTER, ROBARTS RESEARCH INSTITUTE

Baby's first picture is usually not a Kodak moment but a grainy black-and-white sonogram. Such images—generated with ultrasound technology that sends harmless sound waves into the mother's womb and measures what bounces back—usually tax the imagination of anxious parents trying to discern a foot, rump, or face. Images produced with new 3-D ultrasound technology, however, are a marked improvement. The system uses a monitor, computer controls, a processing unit, and a handheld transducer probe, which emits and collects sound waves, to render nose, lips, eyes, fingers, and toes in astonishing detail. It's as if someone photographed a clay model of the fetus.

Ultrasound was first used for clinical diagnosis in 1942 by Austrian psychiatrist and neurologist Karl Dussik. By the 1980s, improvements in microprocessor speed had advanced it into the 3-D arena. Kazunori Baba of the University of Tokyo, Japan, devised the first successful 3-D ultrasound system for obstetrics in 1984; it compiled a series of 2-D "slices" into a 3-D sonogram. But it has really been in the last couple of years that inexpensive computer technology has made it possible to acquire, reconstruct, and display 3-D images quickly, says Aaron Fenster, director and scientist at the Robarts Research Institute's Imaging Research Laboratories in London, Ontario.

Today the technology is being developed by a wide range of companies, including Philips Research, General Electric, and Siemens. Its improved imaging allows doctors to identify or rule out defects such as cleft lips, club feet, and vertebral malformations. "I would expect that in five years, every ultrasound machine in use will have a 3-D option," says Fenster.

Applications for 3-D ultrasound extend outside the realm of obstetrics, too. Radiologists use the technology to locate blood clots in veins and arteries; perform noninvasive breast biopsies on suspicious lesions; diagnose problems in muscles, tendons, or joints; and analyze pains or masses in the abdomen or thyroid. But most people will associate 3-D ultrasound technology with that first glimpse of a new life—the unmistakable faces and features of their yet unborn daughters and sons. TR

For an animated version of this illustration, go to www.technologyreview.com/visualize/.

THINKING LIKE A VIRUS

Why did it take less than two weeks to find the mutant coronavirus responsible for Severe Acute Respiratory Syndrome, or SARS, while it took the better part of three years to find HIV? There are many reasons—including better technology and a less elusive viral target—but don't discount the unprecedented level of worldwide communication among SARS researchers.

The success of a global research network in identifying the pathogen is an example of the huge payoff that can result when researchers put aside visions of patents and glory for their individual laboratories and let their work behave more like, well, a virus. After all, the hallmark of an opportunistic virus like the one that causes SARS is its ability to spread quickly. Those mounting a response need to disseminate their information and innovation just as rapidly.

As you may remember, collaboration was not exactly a strong point in the search for the virus that causes AIDS. That effort, while marked by some remarkable scientific work, was conducted mostly by individual labs working in secret. Pride, prestige, and profit were all very much on the line. So much so, in fact, that Robert Gallo's lab at the National Cancer Institute in the United States wound up in a colossal wrangle for nearly a decade with Luc Montagnier's lab at the Pasteur Institute in Paris over which team had rightful claim to discovering HIV—and which deserved a U.S. patent for an HIV blood test. Montagnier's team even sued the National Cancer Institute, seeking a share of millions of dollars in royalties from a blood test patent garnered by Gallo's team; the lawsuit ended with an out-of-court settlement splitting those royalties. There is no question that the fighting consumed time that could have been spent trying to combat the disease.

Now fast-forward to the early days of the SARS outbreak. This time around, a collaborative research engine was already primed. For years, a team led by Klaus Stohr, a virologist at the World Health Organization, has been readying an international network of laboratories in anticipation of the next pandemic flu strain. This network of 11 labs with high-level biosafety containment facilities in nine countries around the globe swung into action to combat SARS.

Stohr's team activated secure Web sites that could keep the worldwide network of researchers, clinicians, and epidemiologists in constant contact. This communications system was so well designed that researchers could display patient samples and electron microscope pictures in real time to colleagues continents away. Details of each lab's analysis and testing of samples were posted online so researchers could instantly act upon relevant information. In addition, Stohr's team organized daily teleconferences among researchers to discuss progress and obstacles.

The result was that the already considerable intellectual firepower in each lab enjoyed the multiplier effect. Dick Thompson, a former science journalist who is now a communications officer at the World Health Organization responsible for facilitating communication between SARS researchers and disseminating emerging information about the disease to the public, says the advantage of the arrangement was obvious from the first. "People noted how different it was for them to work together," Thompson says, "and it was a boost to everyone."

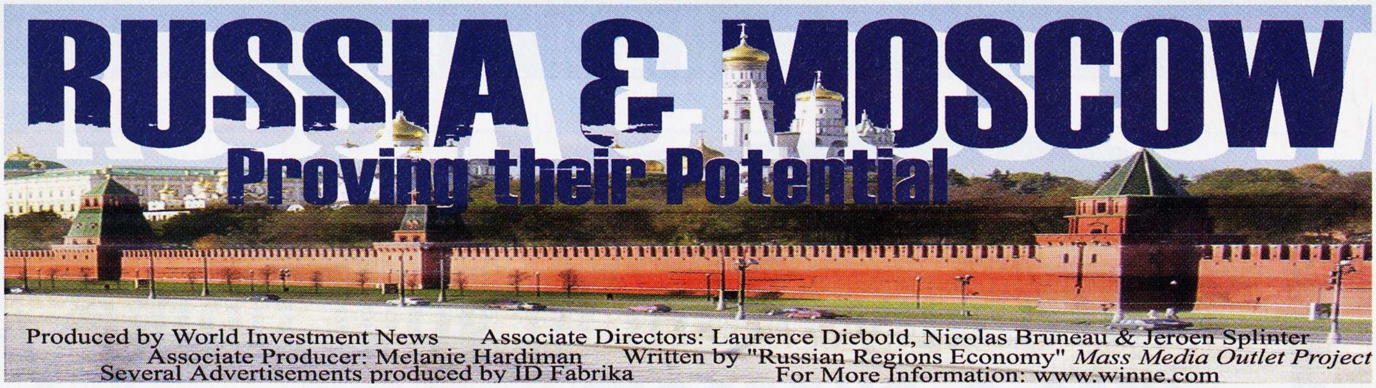
Of course, another benefit of close international teamwork is that an environment of sharing is established from the start that can help prevent the messy kind of patent battle that occurred over the HIV test. In this regard, the research team at the University of Hong Kong that first isolated the SARS virus—led by microbiologist Malik Peiris—deserves special credit for openly sharing its results. The researchers could easily have delayed things by seeking patent rights or public acclaim, but instead, as Thompson notes, "They thought about it for about an hour" and thankfully kept their eyes on the big picture instead.

The researchers hunting for the SARS virus could have delayed progress by seeking patents or public acclaim. Thankfully, they kept their eyes on the big picture, with a huge public health benefit.

Researchers at the U.S. Centers for Disease Control made a similar decision to share their results. Likewise researchers at the British Columbia Cancer Agency, a Canadian government lab in Vancouver, who sequenced the genetic code of the virus and posted it on the Web at dawn on a Sunday so collaborators wouldn't lose a day of research time.

Now, before the letters start pouring in, I know there are all sorts of factors that distinguish the search for HIV from the current SARS endeavor. They include technological advances in fields like DNA analysis; the difficulties posed by HIV, including the lag between infection and the onset of a variety of diseases related to immune deficiency; and the political foot-dragging associated with the perception of AIDS as a disease of homosexuals.

Nonetheless, I still vote for global collaboration as the decisive factor. With all our emphasis on providing incentive for individual innovation, I think we often discount the power of the synergistic effects that can come from spreading innovation around. When fighting a threat like that posed by SARS, it helps to study the enemy's tactics. Let's hope we can continue to spread our ideas at least as rapidly and widely as the most opportunistic virus. TR



Produced by World Investment News Associate Directors: Laurence Diebold, Nicolas Bruneau & Jeroen Splinter
Associate Producer: Melanie Hardiman Written by "Russian Regions Economy" *Mass Media Outlet Project*
Several Advertisements produced by ID Fabrika For More Information: www.winne.com

RUSSIA AND MOSCOW A FUTURE POTENTIAL

Russia is at last entering a period of economic stability. According to Prime Minister Kasyanov "there is a normalization of public life and a step-by-step restoration of the middle class, which suffered the most during the financial crisis of 1998."

ENCOURAGING INVESTMENT & CORPORATE GOVERNANCE

The further development of foreign investment

Mr. Mikhail Krasnov, President of Verysell

is dependant upon the creation of good corporate management practice. Many large companies have an open and transparent economic and financial policy, including a regular dividend issue. Also, successful Russian Initial Public Offerings (IPOs) in the west, such as that offered by GSM-giant VimpelCom, can help improve Russia's blemished corporate and stock market image abroad. Russian investors such as Level 2 Consulting, offering terminals of direct access to NYSE, NASDAQ and AMEX, are also proving that Western markets are not out of reach.

Progress in the financial sector has been made since the 1998 crisis, most notably through the stabilization of the payments system as well as through a disclosure of information bill actively prepared by the government. In 2002 Russia was erased from the Financial Action Task Force's international blacklist of non-cooperative countries.

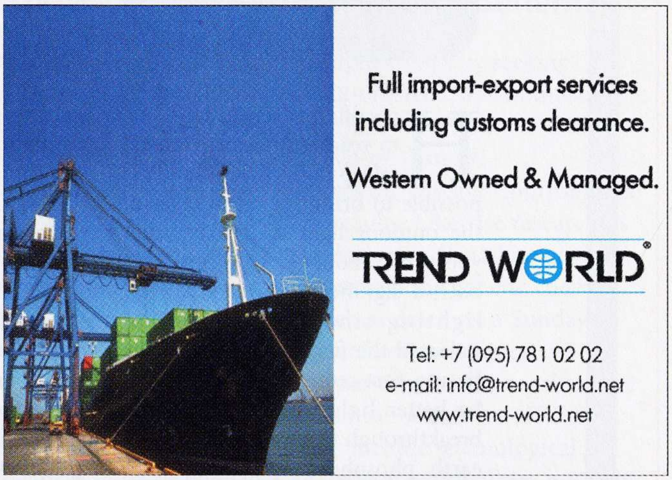
THE POWER SECTOR OPPORTUNITIES IN EQUIPMENT

The privatization of the Unified Energy Systems (UES) and the reorganization of the energy sector dominates the debates, albeit a lack of financing to modernize the industry.

Despite competition from foreign giants as Westinghouse Electric, General Electric and Pratt and Witney, Russian companies have consistently gained strength and market share since 1998. Russian Electrotechnics (RUSEL) is producer of secondary equipment for the energy sector. According to Nenad Popovic, RUSEL President and Chairman of the Board of Directors, "Regarding privatisation, new shareholders and new investors will have to invest in the restructuring of power plants. Therefore, as a producer of secondary equipment we are an excellent partner for these investors".

TELECOMMUNICATIONS CELLULARS LEAD THE WAY

Russia has been reorganizing telecommunications through the enlargement of regional companies in Svyazinvest, a holding company that is 75 percent owned by the state and controls more than 80 regional operators. A real opening to competition cannot be expected before 2010, a date that is tied to Russia's WTO commitments. The Ministry of Communications and Informatization plans to develop the telecommunications market across Russia, and will preserve some restrictions to liberalisation. In order to reach Western standards, the Ministry estimates that Russia will need to accumulate $33 billion in telecommunications investment over the next 10 years. Foreign players should be able to find fertile soil in the cellular industry. Norwegian Telenor, for example, decided to hook up with local



GSM giant, VimpelCom. "While setting up a national network we make sure that it has a unified strategy throughout the country with the same technical solutions, the same billing system, the Same customer service and, of course, the same brand", stresses Jo Lunder, CEO of VimpelCom / Beeline. "The Beeline brand has been linked to innovation and strong performance for Many years", says Lunder with pride. Russia foresees 22.2 million cellular users by 2010.

INFORMATION TECHNOLOGIES PROVING THEIR VALUE

As the most experienced and one of the biggest companies in the Russian IT market, the Verysell Group of Companies has played a very important role in introducing information technologies to Russia's corporate world. Verysell has three businesses: distribution, telecoms and systems integration. "All activities are targeted on taking the best from the leading manufacturers in the west and supplying that technology to the Russian economy", says Mikhail Krasnov, President of Verysell.

MOSCOW THE ACKNOWLEDGED LEADER

The city of Moscow has become the acknowledged leader in modern day economic reforms in Russia, attracting 57 percent of all foreign investment into Russia and accounting for some 28 percent of total Russian goods turnover. However, according to Tamara Vasilieva, CEO and President of Trend-World, provider of customs clearance, transportation, and troubleshooting for foreign companies in Russia, "It is very important in Russia to have the right connections and relations in order to get things done quickly." Today, Moscow's business infrastructure boasts a road network of 4,650 km, 3 inland ports, train stations with an inner-city railroad network of 509 km, an extensive subway system, and finally 5 airports (including international airport Sheremetyevo 2, which includes Aerofirst's duty free shops) that host 53 airlines. Established in 1998, Aerofirst, a joint venture between Aeroflot, Aer Rianta and the Sheremetyevo Airport Authority, was a real breakthrough for Russian customers. The company soon saw itself dominate the market and reach world standards. "We are the absolute leaders of duty free trade in Russia and we hold a flattering position in the world duty free community", Mikhail Dzamashvili, General Director of Aerofirst proudly emphasizes.

In conclusion, Russia is currently living through a period of grace with an economic recovery and a vibrant business community centered around the city of Moscow.

INDEX

PEOPLE AND ORGANIZATIONS MENTIONED IN THIS ISSUE

PEOPLE

Afzal, Omar 40
Bass, Gary 40
Bayes, Thomas 32
Benderson, Ben 26
Conant, James B. 40
Condon, Edward U. 40
Culler, David 50
Davis, Paul 50
Delin, Kevin 50
Desai, Tejal 58
Dirac, Paul 40
Dishman, Eric 22
Epstein, Gerald 40
Estrin, Deborah 50
Fauchet, Philippe 23
Federoff, Howard 24
Fissell, William 58
Foral, Tomas 40
Fuchs, Klaus 40
Gerlach, Jörg 58
Gierke, Tim 26
Glaser, Steven 50
Graham, Paul 32
Heckerman, David 32
Humes, David 58
Judge, Paul 32
Kaiser, William 50
Knowland, William 40
Kordower, Jeffrey H. 24
Kriss, Rick 50
Laffel, Lori 18
Lewis, Jennifer 18
Marburger, John 40
Mazariegos, George 58
McCarthy, Joseph 40
Miller, Larry 19
Mozena, John 32
Nelson, Jay 32
Nunn, Alan 40
Oppenheimer, J. Robert 8
Paganini, Emil 58
Pavel, Misha 22
Perlin, Ken 26
Petrovic, Mark 32
Pierce, John R. 80
Plocher, Tom 22
Poor, Robert 50
Popp, Robert L. 64
Poste, George 40
Pottie, Greg 50
Praed, Jon 32
Prakash, Vipul Ved 32
Ralsky, Alan 32
Reid, Lola 58
Rosengard, Ariella 40
Salem, Enrique 32
Schroth, Lindsay 24
Sergeant, Matt 32
Shein, Barry 32
Smarr, Larry 50
Suga, Hiroaki 28
Tennenhouse, David 50
Travis, Gregory 18
Venter, Craig 40
Wallace, Steven 18
Want, Roy 19
Weisman, Bruce R. 26
Weng, Juyang 64
White, Scott 18
Zhao, Feng 50

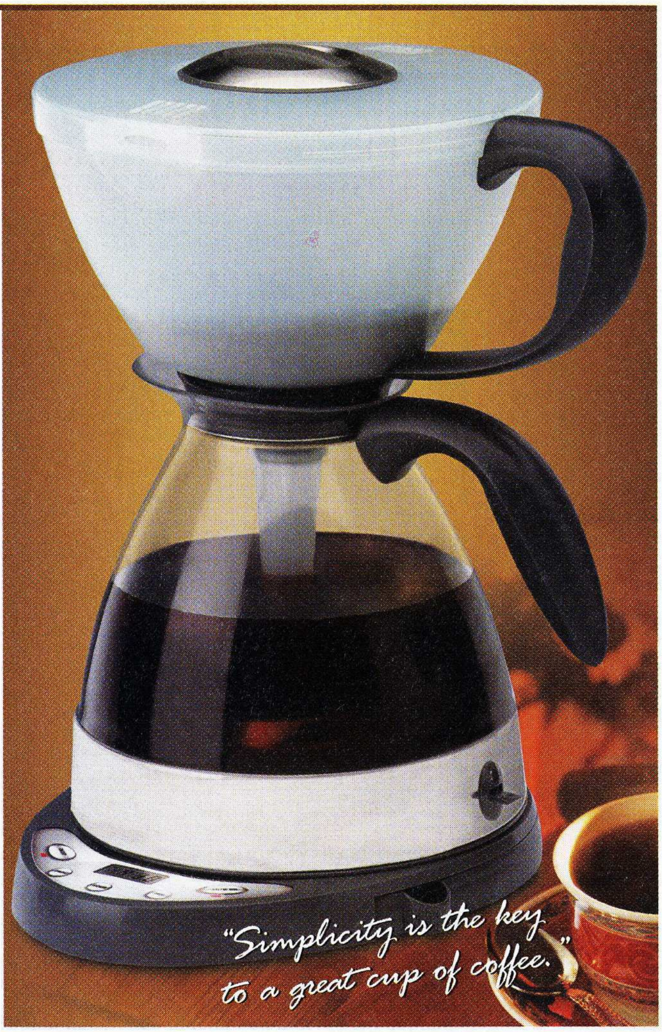
ORGANIZATIONS

Advanced Network Management 18
Anti Spam Research Group 32
AOL 32
Boston University 58
Brightmail 32
California Institute for Telecommunications and Information Technology 50
Celera Genomics 40
China Railcom 24
CipherTrust 32
Cleveland Clinic 58
Cloudmark 32
Coalition against Unsolicited Commercial E-mail 32
Cornell University 40
Crossbow Technology 50
DuPont 26
Dust 50
EarthLink 32
Ember 50
Ferris Research 32
fSONA 24
GeoPhoenix 26
Harvard University 18
Honeywell Laboratories 22
Indiana University 18
Institute for Defense Analyses 40
Intel 19, 22, 50
Internet Law Group 32
Matsushita Electric Works 23
MessageLabs 32
Michigan State University 58
Microsoft 32
Millennial Net 50
MIT 18, 32
Motorola 23
NASA 50
National Institutes of Health 40
National Science Foundation 50
Nephros Therapeutics 58
New York University 26
Oregon Health and Science University 22
Palo Alto Research Center 50
Proxity Digital Networks 18
Radicati Group 32
Rush Presbyterian Medical Center 24
Sana Security 28
Sensicast Systems 50
Sensoria 50
Smith and Hawken 28
Spamhaus Project 32
State University of New York at Buffalo 28
Stottler Henke 19
Terabeam 24
The World 32
University of Arkansas 19
University of California, Berkeley 50
University of California, Los Angeles 50
University of California, San Francisco 24
University of Connecticut 40
University of Maryland 26
University of Michigan 58
University of North Carolina at Chapel Hill 58
University of Pennsylvania 40
University of Pittsburgh 58
University of Rochester 23, 24
University of Texas at Austin 28
U.S. Defense Advanced Research Projects Agency 50, 64
Verizon 32
VidaCare 19
Vitagen 58
Xsilogy 50
Yankee Group 24

CLASSIFIEDS

Vacuum technology brews the perfect cup of coffee…at home

The Infuze™ Vacuum Coffeemaker produces true vacuum-brewed premium coffee in less than 10 minutes.



NEW! Revolutionary technology sold exclusively through TechnoScout

Have you ever wondered what makes a truly great cup of coffee? Part of the answer deals with the quality of the water, and the quality of the bean you use. But the other part has to do with the coffeemaker itself. Where temperature of the water and the amount of time the water is in contact with the coffee grounds are concerned, the Infuze™ Vacuum Coffeemaker steps in to take control and serve you a cup of coffee you'll never forget—every time. If you're a coffee lover, can you imagine how it would be to have a perfect cup of gourmet, robust coffee every single morning? Or serving guests the best coffee they've ever had? It's possible with the remarkable technology of the Infuze™ Vacuum Coffeemaker.

The science of better coffee. The Infuze™ Vacuum Coffeemaker is a unique method for brewing a consistently great cup of coffee. Where ACD's (Automatic Drip Coffeemaker) only have a single pass of hot water for coffee extraction, and percolators re-circulate the water and coffee/water mixture repeatedly, the Infuze has performance/extraction characteristics closely related to the taste of a French Press. Featuring true "vacuum" brewed, premium coffee in under just 10 minutes, the Infuze has a tubular heating element that allows for variable brewing (two to 10 cups). The bottom vessel of the Infuze acts as a removable water reservoir and wide-mouth serving carafe. When brewing, the water is funneled to the top vessel to mix with the grounds after it's been heated. The volumetric/physics calculations of the lower vessel work as a "timer" to keep the hot water and coffee in suspension for a determined period of time that will result in maximum coffee flavor and optimal bean extraction. The coffee is then filtered back down to the lower vessel, while the spent grounds stay up top! With a permanent filter and "soft-grip" handles, the Infuze is easy-to-use, and also easy-to-clean! Just imagine no more annoying paper filters that lose or taint flavorful oils and have to be thrown away! Also comes with a convenient kickstand for storing the top vessel after brewing cycle, and is completely programmable with a digital clock. Dishwasher safe.

The Infuze™ Vacuum Coffeemaker is a unique method for brewing a consistently great cup of coffee.

The Infuze™ Vacuum Coffeemaker controls the water temperature and the time the water is in contact with the beans. It has performance/extraction characteristics closely related to the taste of a French Press.

- *The taste and brewing/extraction performance is unmatched by conventional ACDs (Automatic Drip Coffeemakers) and percolator devices.*
- *Permanent filter—no need for paper filters*
- *True vacuum brewed, premium coffee in under 10 minutes.*
- *Brews 2–10 cups*
- *Easy-to-use, easy-to-clean design*

Flavorful oils are not lost or tainted by paper filters when using the Infuze™ Vacuum Coffeemaker.

Wake up to a great cup of coffee—every morning. Forget mediocre coffee in the morning! It's time to find out for yourself how the innovative technology of the Infuze Vacuum Coffeemaker can serve you an incredible cup of coffee every single morning! The Infuze comes with a 1-year warranty and is backed by TechnoScout's exclusive in-home, 30-day trial. If you aren't completely satisfied by the quality of this high-tech coffeemaker, simply return it within 30 days for the full purchase price.

Infuze™ Vacuum Coffemaker™

ZR-3107………… **$69.95 each** + S&H

Please mention promotional code 24661.

For fastest service, call toll-free 24 hours a day

800-399-7858

To order by mail with check or money order, or by credit card, please call for total amount plus S&H. To charge it to your credit card, enclose your account number and expiration date.

Virginia residents only—please add 4.5% sales tax.

LATEST…GREATEST…NEATEST…COOLEST
You can see hundreds of high-tech products at
www.technoscout.com

TECHNOSCOUT

1998 Ruffin Mill Road
Colonial Heights, VA 23834

33131

COURTESY OF NASA

LIVE VIA SATELLITE

At first, the idea of communications satellites went over like a lead balloon

On August 12, 1960, NASA and Bell Laboratories sent a 30-meter aluminum-coated Mylar balloon into space—launching the satellite communications industry. The project would never have gotten off the ground if it weren't for the persistence of John R. Pierce, a visionary Bell Labs engineer who moonlighted as a science fiction writer.

While Pierce was an electrical engineering student at Caltech, he wrote a science fiction story that took second place in a local contest. After he accepted a job at Bell Labs in 1936, he continued writing under the pseudonym J. J. Coupling. Because Pierce was known for his way with words, in 1948 colleague Walter Brattain asked him for help naming a new device that amplified electrical signals. Pierce suggested "the transistor," and the name stuck.

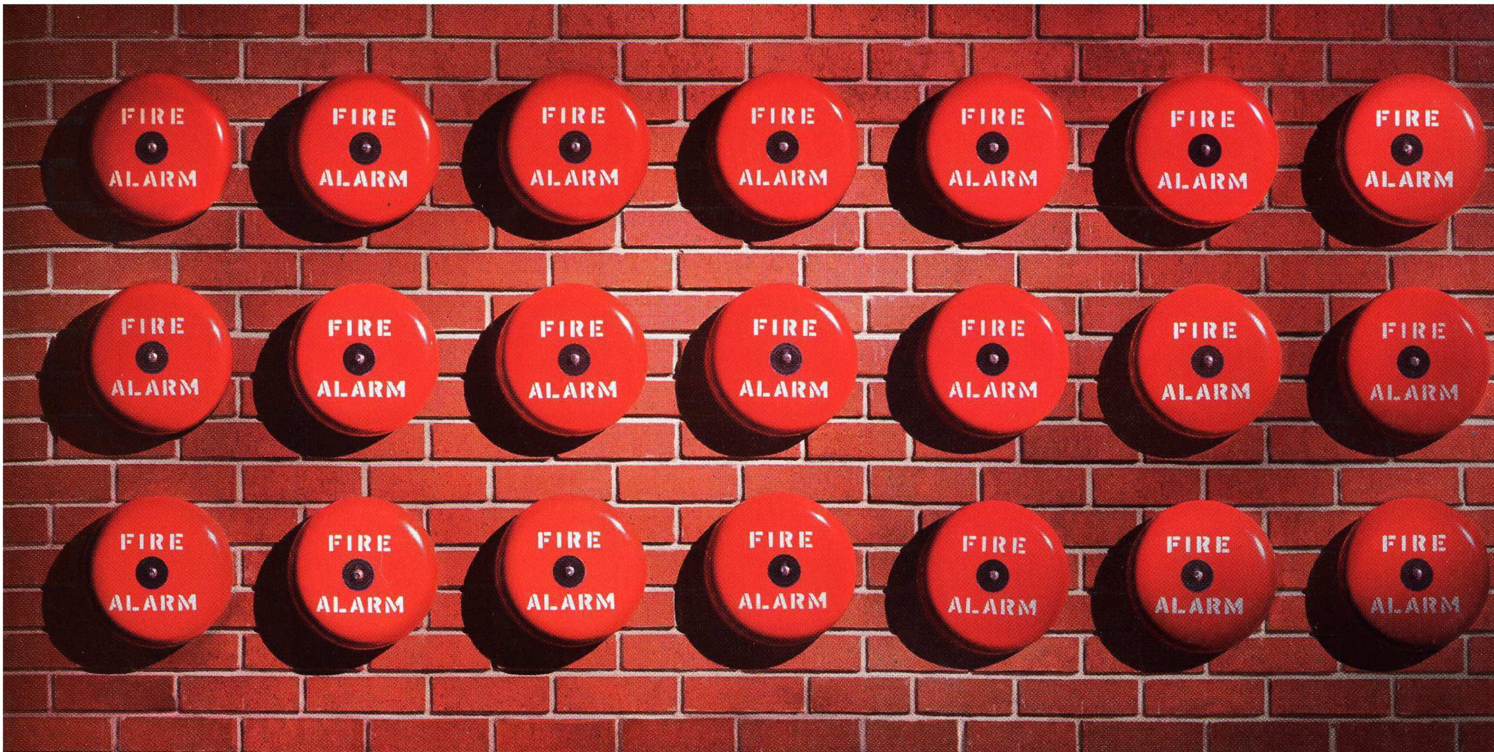
In 1952, the year Pierce became Bell Labs' director of electronics research, he wrote an article in which he calculated the power necessary to transmit signals across wide distances via large balloon-type satellites. Over the next several years, he gave lectures and published scientific papers on communications satellites but wasn't able to convince Bell Labs to pursue the potentially costly project.

Pierce finally had a lucky break when he discovered that William J. O'Sullivan, an aeronautical engineer at NASA, had built a large metallic balloon of the kind he had envisioned—although O'Sullivan planned to use it to measure atmospheric density, not to reflect communications signals across the world.

In 1959, NASA and Bell Labs agreed to collaborate on a balloon satellite, in what became known as Project Echo. NASA would provide and launch the balloon, its Jet Propulsion Laboratory at Caltech would build a West Coast station to send signals, and Bell Labs would construct an East Coast receiving station. On that August day in 1960 when Echo I was successfully launched, a recorded message from President Eisenhower was transmitted from Goldstone, CA, to the Bell Labs station in Crawford Hill, NJ.

Echo I orbited the globe for eight years before finally falling back to earth. Pierce himself retired from Bell Labs in 1971 and in 1983 became a visiting professor of music at Stanford University. Pierce died on April 2, 2002, at age 92. His original satellite would have many successors: 2001 alone saw 39 communications satellite launches worldwide. Today, more than 150 communications satellites circle the globe, transmitting everything from phone calls to Global Positioning System data. *—Lisa Scanlon*

Technology Review (ISSN 1099-274X), Reg. U.S. Patent Office, is published monthly, except bimonthly in December/January and July/August, by the Massachusetts Institute of Technology. Entire contents ©2003. The editors seek diverse views, and authors' opinions do not represent the official policies of their institutions or those of MIT. Printed by Brown Printing Company, Waseca, MN. Periodicals postage paid at Boston, MA, and additional mailing offices. Postmaster: send address changes to *Technology Review*, Subscription Services Dept., PO Box 420005, Palm Coast, FL 32142 , or via the Internet at www.technologyreview.com/customerservice/. Basic subscription rates: $34 per year, Canadian residents add $10, other foreign countries add $30. Publication Mail Agreement Number 40621028. Send undeliverable Canadian copies to PO Box 1051, Fort Erie, ON L2A 6C7. Printed in U.S.A.
ABC audited



MORE SECURITY DOESN'T MAKE YOU MORE SECURE.

BETTER MANAGEMENT DOES.

The secret to a secure enterprise lies in not just monitoring the parts, but managing it as a whole. That's exactly what *e*Trust™ lets you do. In fact, our *e*Trust™ Security Command Center is the perfect solution to security information overload. It gives you the big picture from a single vantage point, with all your event information prioritized. So you can identify actual internal and external threats before they can wreak havoc. Anything less would be, well, alarming.

For more information on security management, go to ca.com/etrust/management.

*e*Trust™ | ACCESS • THREAT • IDENTITY SECURITY MANAGEMENT SOFTWARE | Computer Associates®


QUADRASTEER
2003 GMC YUKON XL
THE YUKON XL WITH OPTIONAL QUADRASTEER™ BY DELPHI IS THE FIRST SUV THAT ENABLES THE REAR WHEELS TO ACTUALLY STEER ALONG WITH THE FRONT. AT LOW SPEEDS, THE BACK WHEELS TURN IN THE OPPOSITE DIRECTION, GIVING THIS 8-SEATER THE TURNING CIRCLE OF A COMPACT CAR. OVER 45 MPH, ALL FOUR WHEELS STEER IN THE SAME DIRECTION. TIGHT SPACES? TOWING? LANE CHANGING? NOT A PROBLEM. PROFESSIONAL GRADE ENGINEERING. IT'S NOT MORE THAN YOU NEED. JUST MORE THAN YOU'RE USED TO.
WE ARE PROFESSIONAL GRADE.™
GMC
"FITS LIKE A GLOVE."
- ASTONISHED PARKING LOT ATTENDANT AS HE BACKS YOUR SUV INTO A 20-FOOT SPACE
YUKON XL
Yukon and GMC logo are registered trademarks of the General Motors Corporation. ©2003 General Motors Corp. All rights reserved.